Bureau of Prisons, United States Department of Justice, HOLC Building, 320 First Street., NW., Washington, DC 20534
Community Relations Service, United States Department of Justice, 5550 Friendship Boulevard, Chevy Chase, MD 20815
Drug Enforcement Administration, Eye Street Building, 1405 Eye Street, NW., Washington, DC 20005
Executive Office for Immigration Review, United States Department of Justice, 5203 Leesburg Pike, Falls Church, VA 22041
Executive Office for United States Attorneys
Executive Office for United States Trustees, United States Department of Justice, HOLC Building, 320 First Street, NW., Washington, DC 20534
Federal Bureau of Investigation, 9th St. & Pennsylvania Ave., NW., Washington, DC 20535 [for field offices, consult the list of FBI field offices in the United States Government Manual]
Federal Prison Industries, Inc., HOLC Building, 320 First Street, NW., Washington, DC 20534
Foreign Claims Settlement Commission, Vanguard Building, 1111 20th Street, NW., Washington, DC 20579
Immigration and Naturalization Service, 425 Eye Street, NW., Washington, DC 20536 [for district offices consult the list of INS district offices in the United States Government Manual]
Office of Intelligence Policy and Review
Office of the Pardon Attorney, United States Department of Justice, Park Place Building, 5550 Friendship Blvd., Chevy Chase, MD 20815
Office of Professional Responsibility
Office of Public Affairs
United States Marshals Service, One Tysons Corner Center, McLean, VA 22102
United States National Central Bureau—Interpol
United States Parole Commission, Park Place Building, 5550 Friendship Blvd., Chevy Chase, MD 20815

Field Offices

Antitrust Division:

Richard B. Russell Building, 75 Spring Street, SW., Suite 1394, Atlanta, Georgia 30303, (404) 331–7100
John C. Kluczynski Building, 230 South Dearborn Street, Room 3820, Chicago, Illinois 60604, (312) 353–7530
995 Celebrezze Federal Building, 1240 East 9th Street, Cleveland, Ohio 44199–2089, (216) 522–4070
Earle Cabell Federal Building, 1100 Commerce Street, Room 8C6, Dallas, Texas 75242, (214) 767–8051
26 Federal Plaza, Room 3630, New York, New York 10278–0096, (212) 264–0390
11400 U.S. Courthouse, 601 Market Street, Philadelphia, Pennsylvania 19106, (215) 597–7405
450 Golden Gate Avenue, Box 36046, San Francisco, California 94102, (415) 556–6300

[Order No. 1055–84, 49 FR 12263, Mar. 29, 1984; Order 1215–87, 52 FR 34214, Sept. 10, 1987]

PART 17—REGULATIONS IMPLEMENTING EXECUTIVE ORDER 12356, "NATIONAL SECURITY INFORMATION"

Subpart A—General Provisions

Subpart B—Security Classification

Subpart C—Declassification and Downgrading

Subpart D—Identification and Marking

Subpart E—Safekeeping and Storage

Subpart F—Foreign Government Information

Subpart G—Access, Dissemination, and Accountability

AUTHORITY: 5 U.S.C. 301; 28 U.S.C. 509, 510; E.O. 12356.

SOURCE: Order No. 1112–85, 50 FR 46388, Nov. 7, 1985, unless otherwise noted.

Subpart A—General Provisions

§17.1 Purpose.

The purpose of this regulation is to insure that information within the Department of Justice, herein referred to as the Department, relating to the national security (as used hereinafter, a collective term which means the national defense and foreign relations of the United States) is protected, pursuant to the provisions of Executive Order 12356 and its implementing directive. (See §17.2 (a) and (b)). This regulation prescribes: a progressive system for classification, downgrading and declassification; information safeguarding policies and procedures; a monitoring system to insure the effectiveness of the National Security Information Program throughout the Department; and a system for reporting and investigating security violations and sanctions for such violations. The provisions of this regulation become effective upon approval by the Attorney General.

§17.2 Authority.

(a) This regulation is issued in compliance with, and as a supplement to, the provisions of:

(1) 28 U.S.C. 503 and 509;

(2) 5 U.S.C. 301;

(3) Executive Order No. 12356 entitled, ''National Security Information,'' dated April 2, 1982.

(4) Director of Central Intelligence Directive Number 1/14 entitled, ''Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information.''

(5) The Information Security Oversight Office Directive No. 1 entitled, ''National Security Information,'' dated June 23, 1982.

(6) 28 CFR 0.75(p), which outlines the security policy functions of the Justice Management Division (Security Staff).

(7) Department Order 2600.2A entitled, ''Security Programs and Responsibilities.''

(b) *List of references.* (1) Department Order 2620.4 entitled, ''Physical Security Manual for Safeguarding Classified National Security Information (E.O. 11652).''

(2) Department Order 2620.6 entitled, ''Procedures for Requesting a Department of Justice Security Clearance for Non-Contractor Personnel Outside the Executive Branch.''

(3) Department Order 2600.3A entitled, ''Requirements for Safeguarding Classified Information and Material Released to Industry in Connection with Contracts or Grants.''

(4) Department Order 2660.1A entitled, ''Department of Justice Special Security Center (Room 6744—Main Justice).''

(5) Offices, Boards and Divisions (OBD) Order 2710.3A entitled, ''Files Maintenance and Records Disposition.''

§ 17.3 Applicability.

This regulation governs the Department's National Security Information Program and takes precedence over all Department publications affecting that program. It establishes, for uniform application throughout the Department, the policies, standards, criteria and procedures for the classification, downgrading, declassification and safeguarding of National Security Information originated, produced or handled by, or in the custody of, the Department.

§ 17.4 Application to non-Executive Branch personnel.

Except as otherwise provided herein (see § 17.96), the provisions of this regulation apply to non-contractor personnel outside of the Executive Branch and to contractor personnel or employees who are entrusted with National Security Information originated within or in the custody of the Department. Clearance procedures for the aforementioned personnel are contained in Department Orders 2620.6 and 2600.3A, respectively. Procedures for clearing Department personnel are contained in § 17.98 of this regulation.

§ 17.5 Atomic Energy Act.

Nothing in this regulation supersedes any requirements made by or under the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011–2394. ''Restricted Data'' shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2161–2166, and the regulations issued pursuant thereto.

Subpart B—Security Classification

§ 17.6 Policy.

(a) Except as provided in § 17.5, Executive Order 12356, as implemented by this regulation, provides the only basis for classifying information.

(b) Unnecessary classification and higher than necessary classification shall be scrupulously avoided.

(c) Classification shall be continued no longer than is necessary for the protection of national security.

(d) Information may not be classified except for the purposes of preventing damage to the national security.

§ 17.7 Classification levels.

(a) *General.* Official information which requires protection against unauthorized disclosure in the interests of national security shall be classified in one of three levels, namely, ''Top Secret,'' ''Secret'' or ''Confidential.'' No other terms shall be used to identify official information as requiring protection in the interests of national security, except as otherwise expressly provided by statute.

(b) *Top Secret.* ''Top Secret'' is the designation which shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of ''exceptionally grave damage'' could include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of extremely sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with restraint.

(c) *Secret.* ''Secret'' is the designation which shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of ''serious damage''

could include disruption of foreign relations affecting the national security; impairment of a program or policy directly related to the national security; revelation of military plans or intelligence operations; and compromise of scientific or technological developments relating to national security.

(d) *Confidential.* ''Confidential'' is the designation which shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security. Examples of damage could include the compromise of information which indicates strength of armed forces in the United States and overseas areas; disclosure of technical information used for intelligence operations; a written inspection report of classified areas; revelation of performance characteristics, test data, design, and production data on intelligence gathering equipment.

§17.8 Original classification authority.

Authority for original classification of information as Top Secret, Secret or Confidential may be exercised only by the Attorney General and by officials to whom such authority is specifically delegated in accordance with and subject to the restrictions of this section. In the absence of an authorized classifier, the person designated to act in his or her absence may exercise the classifier's authority.

(a) *Top Secret.* Only the Attorney General or the Assistant Attorney General for Administration may delegate original Top Secret classification authority. Such delegation may only be made to principal subordinate officials who are determined to have frequent need to exercise such authority. The delegation of authority must specify whether the Top Secret classification authority is authorized to delegate original Secret and Confidential classification authority.

(b) *Secret and Confidential.* Only the Attorney General, the Assistant Attorney General for Administration and officials with delegated original Top Secret classification authority who are specifically authorized in writing to do so may delegate original Secret and Confidential classification authority to subordinate officials whom they determine to have frequent need to exercise such authority.

(c) A request for delegation of original classification authority pursuant to section 1.2 of Executive Order 12356 original classification authority shall be in writing. The Department Security Officer shall maintain a current listing of officials delegated original classification authority by name, position, or other identifier. If possible, the listing shall be unclassified.

(d) Except for the Attorney General and the Assistant Attorney General for Administration, officials to whom original classification authority is delegated may not, under any circumstances, redelegate such authority. However, those officials so designated by the Attorney General may delegate a lesser level of classification authority.

(e) Annual reviews, and special review as requested by the Department Security Officer, shall be made by Security Programs Managers to ensure that those to whom such authority has been delegated have demonstrated a continuing need to exercise it. the annual reviews are to be conducted at the end of each calendar year. Findings of this review are to be forwarded to the Department Security Officer.

§17.9 Propriety of classification actions.

In accordance with §17.144, all personnel assigning classifications to information within the Department are accountable for the propriety of such classifications, whether in the exercise of original classification authority or in the determination and application of classifications assigned in source documents or classification guides (i.e., derivative classification), and are required to maintain adequate records to support their classification actions.

§17.10 Challenges to classification.

(a) Improper classification actions shall be reported initially by the holder of the information to the appropriate Security Programs Manager within the Department. The Security Programs Manager must report each case of improper classification within his/her

area of concern to the Department Security Officer. Cases of improper classification, if willful and knowing, must then be reported to the Director of the Information Security Oversight Office.

(b) If holders of classified information have reason to believe that the information is classified improperly or unnecessarily or that an overly restrictive period for continued classification has been assigned, they are encouraged to challenge such classification with their Security Programs Manager or the classifier of the information, with a view to bringing about corrections.

§ 17.11 Accounting for classification actions.

The Department Security Officer shall establish, in coordination with the Information Security Oversight Office, a system for maintaining information on classification actions within the Department.

§ 17.12 Identification of classification authority.

Information classified under the provisions of this regulation shall indicate on its face, in the case of documents, or by notice or other means, in the case of material, the identity of the classifier. Such identification shall be shown on the ''CLASSIFIED BY'' line. In those cases where the personal identity of the authorized classifier would be classifiable, an alternate identification method may be used provided it is approved by the Department Security Officer.

§ 17.13 Derivative classification.

(a) Information extracted or derived from a classified source document or classification guide and used in a Department originated document will be classified, or not classified, as the case may be, in accordance with the classification guide or source document. The overall marking and paragraph marking of the source document should supply adequate classification guidance to the person making the extraction.

(b) If a person who applies derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult for a determination an appropriate official of the originating agency or office of origin who has the authority to upgrade, downgrade, or declassify the information.

(c) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(d) Persons who apply derivative classification markings shall:

(1) Observe and respect original classification decisions; and

(2) Carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

(e) If paragraph markings are lacking, and when no classification guidance is included in the source document and no reference is made to an applicable classification guide which is available for use by the person making the extraction, the extracted or derived information will be classified in accordance with guidance specifically sought and received from the original classifier of the source material. If such guidance cannot be obtained, the information or material will be given the classification which corresponds to the overall marking of the source document.

§ 17.14 Positive judgment requirement.

Classification is a positive judgment, i.e., there must be a reasonable basis for classification. All principles and criteria within this subpart must be considered before classification determination is made or a classification marking is applied. If there is reasonable doubt about which classification designation is appropriate, the information will be safeguarded at the higher level of classification until a determination, which shall be made in 30 days, is made by the original classification authority. If there is reasonable doubt about whether the information should be classified at all, it shall be

safeguarded as if it were ''Confidential'' information pending the determination about its classification which shall be made by the original classification authority within 30 days.

§17.15 Classification in context of related information.

Certain information which would otherwise be unclassified may require classification when combined or associated with other classified or unclassified information, including that which the classifier knows already has been officially released into the public domain.

§17.16 Classification categories.

(a) A determination to classify may be made only if the information concerns one or more of the categories in paragraph (b) of this section and if the unauthorized disclosure of the information reasonably could be expected to cause damage to the national security.

(b) Information must be considered for classification if it concerns:

(1) Military plans, weapons, or operations;

(2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) Foreign Government Information;

(4) Intelligence activities (including special activities), sources or methods;

(5) Foreign relations or foreign activities of the United States;

(6) Scientific, technological, or economic matters relating to the national security;

(7) U.S. Government programs for safeguarding nuclear materials or facilities;

(8) Cryptology;

(9) A confidential source; or

(10) Other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President by a person designated by the President or by the Attorney General. Requests for any such additional category of information shall be forwarded through the Department Security Officer and the Assistant Attorney General for Administration to the Attorney General for approval. Any additional categories of information approved by the Attorney General must be reported promptly to the Director of the Information Security Oversight Office.

§17.17 Duration of classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official who has classification authority over the information. Any decision to extend an automatic declassification shall be made with respect to individual documents or categories of information. The Department is responsible for notifying holders of the information of such extensions. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Department Security Officer.

(c) Information marked for declassification review under predecessor orders shall remain classified until reviewed for declassification under the provisions of this regulation.

§17.18 Classification of Foreign Government Information.

(a) Unauthorized disclosure of Foreign Government Information or the identity of a confidential foreign source is presumed to cause damage to the national security and, accordingly, such information shall normally be assigned a classification of at least ''Confidential.''

(b) If the fact that information is Foreign Government Information must be concealed, a marking shall not be used and the document shall be marked as if it were wholly of United States origin.

§17.19 Prohibitions.

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization or agency; or to restrain competition. Information may be classified, notwithstanding that it

falls within the otherwise prohibited categories of this subsection, if disclosure would result in damage to the national security as set forth in §17.7.

(b) Classification may not be used to prevent or delay the release of information that does not require protection in the interest of national security.

(c) Basic scientific research information not clearly related to the national security may not be classified.

(d) Information may not be classified unless it is owned by, produced by or for, or is under the control of the U.S. government. This prohibition does not affect the provisions of chapter 17 of title 35 U.S. Code.

(e) References to classified documents, when such references do not disclose classified information, may not be classified or used as a basis for classification.

(f) Information may be classified or reclassified after receipt of a request for it under the Freedom of Information Act or the Mandatory Review provisions of this regulation (subpart C) if such classification is consistent with this regulation and is authorized by the Attorney General, the Deputy Attorney General, the Assistant Attorney General for Administration or an official with Top Secret classification authority. Classification authority under this provision shall be exercised personally, on a document-by-document basis.

(g) Markings other than ''Top Secret,'' ''Secret,'' or ''Confidential,'' such as ''For Official Use Only,'' ''Limited Official Use'' or ''Eyes Only,'' shall not be used to identify National Security Information. No other term or phrase shall be used in conjunction with these markings, such as ''Secret Sensitive'' or ''Agency Confidential,'' to identify National Security Information. The terms ''Top Secret,'' ''Secret,'' and ''Confidential'' should not be used to identify nonclassified Executive Branch information.

§17.20 Effect of open publication.

Appearance in the public domain of information currently classified or being considered for classification does not preclude initial or continued classification. However, such disclosures require reevaluation of the information to determine whether the publication has been compromised to the degree that downgrading or declassification is required. Similar consideration must be given to related items of information in all programs, projects, cases or items incorporating or pertaining to the compromised items of information. Holders should continue classification until advised to the contrary by a competent Government authority.

§17.21 Classification of previously declassified information.

(a) Declassified information, once communicated as such to a member of the public, may be reclassified only when an authorized official determines in writing that:

(1) The information requires protection in the interest of national security; and

(2) The information may be reasonably retrieved either voluntarily or by litigation from the persons not approved for access.

(b) In addition, before reclassifying the information, the authorized official must consider:

(1) The elapsed time following disclosure;

(2) The nature and extent of the disclosure;

(3) The ability to bring the fact of reclassification to the attention of persons to whom the information was disclosed; and

(4) The ability to prevent further disclosure.

(c) All reclassifications of information previously declassified and disclosed must be reported promptly to the Department Security Officer. This information must then be reported by the Department Security Officer to the Director of the Information Security Oversight Office.

§17.22 Requirement for issuance of classification guides.

(a) Executive Order 12356 requires that classification guides be prepared to facilitate the proper and uniform derivative classification of information by those heads of an Office, Board, Division or Bureau having original classification authority. Such guides shall be

issued based upon classification determinations made by appropriate classification authorities in coordination with the Department Security Officer.

(b) Each classification guide must be approved personally and in writing by the Assistant Attorney General for Administration or an official who:

(1) Has program or supervisory responsibility over the information; and

(2) Is authorized to classify information originally at the highest level of classification contained in the guide.

§17.23 Waiver of classification guide requirements.

(a) The Attorney General may for good cause grant and revoke waivers for classification guides for specified classes of documents or information. Any waivers granted shall be reported through the Department Security Officer to the Director of the Information Security Oversight Office.

(b) The decision to waive the requirement to issue classification guides will be based, at a minimum, on an evaluation of the following factors:

(1) The ability to segregate the specified classes of information;

(2) The impracticality of producing the guide because of the nature of the information;

(3) The anticipated lack of usage of the guide as a basis for derivative classification; and

(4) The availability of alternative sources for classifying the information in a uniform manner.

§17.24 Classification guide components.

Classification guides shall:

(a) Identify the information elements to be protected, using categorization and subcategorization to the extent necessary to ensure that the information involved can be readily and uniformly identified.

(b) State which of the classification designations, i.e., Top Secret, Secret, or Confidential apply to the identified information.

(c) State the declassification instructions for each element or category of information in terms of a period of time, future event, or a notation that the information shall not be automatically declassified without the approval of the originating agency.

§17.25 Review of classification guides.

Classification guides shall be reviewed for currency and accuracy not less than once every two years. If no changes are made, the originator or his representative shall so annotate the record copy and show the date of the review. A listing of all Department classification guides in use shall be maintained by the Department Security Officer.

§17.26 Emergency classification authority.

(a) When an employee, contractor, licensee or grantee not authorized to classify National Security Information within the Department originates or develops information which requires immediate classification and safeguarding and no authorized classifier is available, that person shall:

(1) Safeguard the information in the manner prescribed for the intended classification.

(2) Mark the information (or cover sheet if applicable) with the appropriate classification.

(3) Transmit the information within five working days to the organization that has appropriate subject matter interest and classification authority. If it is not clear which organization has classification responsibility for this information, it shall be sent to the Department Security Officer. The Department Security Officer shall determine the organization having primary subject matter interest and forward the information with appropriate recommendations to that organization for a classification determination.

(b) When designating information as classified with such security classification markings, the requirements pertaining to overall classification markings contained in this regulation shall be followed.

(c) The organization with classification authority shall decide within 30 days whether to classify this information.

§17.27 Emergency action.

If an emergency requires immediate communication of information believed

to require classification, such information may be transmitted after taking the action prescribed in §17.26. Care shall be taken that the security clearance of the person to whom the classified material or information is being transmitted is correspondent to or higher than the initial classification, in accordance with the provisions of subpart G of this regulation. Additionally, the means of transmission shall be commensurate with the level of the initial classification, as prescribed in subpart G.

§ 17.28 Raising to a higher level of classification.

The upgrading of classified information to a higher level than previously determined, by officials with appropriate authority, shall be followed by prompt notification to all known holders of the information.

§ 17.29 Classification of previously unclassified information.

Unclassified information, once communicated as such, may be classified only when a classifying authority satisfies the requirements described for upgrading in §17.28 and determines that control of the information has not been lost by public dissemination or access.

§ 17.30 Notification.

Prompt notification of all upgrading and unscheduled downgrading actions shall be provided to all known holders of the information.

Subpart C—Declassification and Downgrading

§ 17.31 Policy.

Information shall be declassified or downgraded as soon as national security considerations permit. The Department shall coordinate its review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by §17.16 despite the passage of time will continue to be protected in accordance with this regulation.

§ 17.32 Authority.

(a) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the Attorney General or the Assistant Attorney General for Administration.

(b) The Department Security Officer shall ensure that a current listing of officials delegated declassification authority as prescribed in paragraph (a) of this section is maintained. If possible, this listing will be unclassified.

§ 17.33 Declassification by the Director of the Information Security Oversight Office.

If the Director of the Information Security Oversight Office determines that Department information is classified in violation of Executive Order 12356, the Director may require the information to be declassified by the Department. Any such decision by the Director may be appealed to the National Security Council, through the Department Review Committee. The information shall remain classified until the appeal is decided.

§ 17.34 Systematic review for declassification.

Executive Order 12356 requires the Archivist of the United States, in accordance with established procedures, to conduct systematic reviews for declassification of classified information accessioned into the National Archives and classified Presidential papers and records under control of the Archivist.

§ 17.35 Systematic review responsibilities.

(a) The Attorney General shall:

(1) Issue guidelines to assist the Archivist of the United States for systematic declassification review and, if applicable, downgrading of classified information originated by the Department. These guidelines shall be developed in consultation with the Archivist and the Director of the Information Security Oversight Office;

(2) Designate experienced personnel to provide timely assistance to the Archivist in the systematic review process; and

(3) Review and update guidelines for systematic declassification review and downgrading at least every five years unless earlier review is requested by the Archivist.

(b) The Attorney General may issue, in consultation with the Archivist of the United States and the Director of the Information Security Oversight Office, specific systematic declassification review guidelines for Foreign Government Information over which the Attorney General has declassification authority. These guidelines shall be reviewed and updated every five years unless earlier review is requested by the Archivist.

(c) The Department may conduct internal systematic review programs for classified information originated by its organizations contained in records determined by the Archivist of the United States to be permanently valuable but that have not been accessioned into the National Archives of the United States.

§17.36 Systematic review procedures.

(a) Only permanently valuable records shall be subjected to systematic review for declassification. Classified nonpermanent records that are scheduled to be retained for more than 30 years need not be systematically reviewed, but shall be reviewed for declassification upon request.

(b) The Attorney General, through the Department Security Officer, shall require that all classified records 30 years old or older, whether held in storage areas under Department control or in Federal Records Centers, be surveyed to identify those that require scheduling for future disposition. The Security Programs Managers and Records Management Officials shall coordinate this effort with the Department Security Officer and Department Records Management Officials, respectively.

(c) All Department information accessioned into the National Archives and Records Service that is permanently valuable and more than 30 years old is to be systematically reviewed for declassification by the Archivist of the United States (using the guidelines issued pursuant to §17.35(a)) with the assistance of the Department's personnel designated for that purpose pursuant to §17.35.

(d) The Security Programs Managers shall receive from the Archivist of the United States information which requires the originating agency's determination for declassification or information which the Department's systematic review guidelines state shall not be automatically declassified after 30 years without review by the Department. Security Programs Managers within the Office, Board, Division or Bureau with primary jurisdiction over the classified information either received from the Archivist or in the Office, Board, Division or Bureau's custody, over 30 years old, shall proceed as follows:

(1) Classified information over which the Office, Board, Division or Bureau exercises exclusive or final original classification authority and which, in accordance with the systematic review guidelines developed under this section, is to be declassified, shall be marked and handled as such.

(2) Classified information over which the Office, Board, Division or Bureau exercises exclusive or final original classification authority, and which the head of such organization recommends should be kept protected, shall be identified under appropriate category headings.

§17.37 Mandatory review for declassification.

(a) Upon request by a U.S. citizen, a permanent resident alien, a Government agency or a State or local government to declassify and release information classified under the provisions of Executive Order 12356, such information shall be subject to mandatory review by the originating Office, Board, Division or Bureau for possible declassification in accordance with the procedures of this subpart.

(b) Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in

accordance with special procedures issued by the Secretary of Defense or the Director of Central Intelligence.

(c) The Department, upon conducting a mandatory review for declassification, shall declassify information no longer requiring protection under this regulation. This information will be released unless withholding is otherwise authorized under applicable law.

§ 17.38 Mandatory review for Presidential papers.

(a) Information which was originated by the President, the White House Staff, by committees, commissions or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of the President is exempted from mandatory review for declassification under the provisions of § 17.37.

(b) Information described in § 17.38(a) that is under control of the Archivist of the United States or the Administrator of the General Services Administration is subject to review by the Archivist for declassification or downgrading. This review will be in accordance with procedures developed by the Archivist which shall provide for consultation with the Department in matters of primary subject interest to this Department.

(c) Decisions by the Archivist of the United States may be appealed to the Director of the Information Security Oversight Office. When the Department has primary subject matter interest, it shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

§ 17.39 Mandatory review for Foreign Government Information.

Except as provided in this section, the Department shall process mandatory declassification review requests for classified records containing Foreign Government Information in accordance with § 17.41. The agency that initially received or classified the Foreign Government Information shall be responsible for making a declassification determination after consultation with concerned agencies. If the Office, Board, Division or Bureau receiving the request did not originally receive or classify the Foreign Government Information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request. See subpart F for additional procedures for Foreign Government Information.

§ 17.40 Submission of requests for mandatory review.

Requests for mandatory review of classified information shall be submitted in accordance with the following procedures.

(a) Requests for mandatory declassification review under this subpart shall be submitted to the Director, Office of Information and Privacy, Office of Legal Policy, 10th and Constitution Avenue, NW., Washington, DC 20530. The Office of Information and Privacy shall promptly forward such requests to the Office, Board, Division or Bureau concerned, provided:

(1) A department (any agency of the Government or other governmental unit) or employee thereof, or a U.S. citizen or permanent resident alien requests the review.

(2) The request is in writing and reasonably describes the classified information or material with sufficient particularity to enable the Department to identify it.

(3) The classified information or material can be located with a reasonable amount of effort.

(b) When the description in a request is deficient, the requester should be asked to provide as much additional identifying information as possible. Before denying a request on the basis that the information or material is not obtainable with a reasonable amount of effort, the requester should also be asked to limit his request to information or material that is reasonably obtainable. If the requester then fails to describe the information or material he seeks with sufficient particularity, or if it cannot be obtained with a reasonable amount of effort, the requester shall be notified of the reasons why no action will be taken and of his right to

appeal the decision to the Department Review Committee.

(c) The Office of Information and Privacy shall assign the request to the appropriate Office, Board, Division or Bureau within the Department for action, and shall immediately acknowledge receipt of the request to the requester in writing. The Office, Board, Division or Bureau concerned shall thereafter make a determination within 60 days of receipt of the request or shall explain to the requester the reasons why further time is necessary (including where consultation with other agencies is required pursuant to §17.46(b)). Unless there are unusual circumstances, the Department will make a final decision within one year from receipt of the request. If at the end of one year from receipt of the request for review no determination has been made, the requester may apply to the Department Review Committee for a determination.

(d) If the Office, Board, Division or Bureau determines that continued classification is required, the requester shall promptly be notified, and, whenever possible, provided with a brief statement as to why the requested information or material cannot be declassified. The requester may appeal any such determination to the Department Review Committee and the notice of determination shall advise him of this right. If, after appeal by the requester, the Department Review Committee determines that continued classification is required, it shall promptly notify the requester.

(e) After review, the information or any reasonably segregable portion thereof that no longer requires protection under this regulation shall be declassified and released to the requester unless withholding is otherwise warranted under applicable law. If the information, although declassified, is withheld, the requester shall be given a brief statement as to the reasons for denial and a notice of the right to appeal the determination to the Office of Information and Privacy.

(f) Appeals are to be sent to the Office of Information and Privacy, Office of Legal Policy, 10th and Constitution Avenue, NW., Washington, DC 20530. All appeals of denials must be filed with the Department within 60 days in order to be considered and each notification to a requester must contain a notice to that effect.

(g) In making its determinations concerning requests for declassification of classified information, the Department Review Committee shall impose, for administrative purposes, the burden of proof on the originating Office, Board, Division or Bureau to show that continued classification is warranted.

(h) Requests for declassification which are submitted under the provisions of the Freedom of Information Act, or Privacy Act of 1974, shall be processed in accordance with the provisions of those Acts.

§17.41 Information classsified by agencies other than the Department subject to mandatory review.

(a) When the Office, Board, Division or Bureau receives a request from the Office of Information and Privacy for information in Department custody that involves information classified by another agency, it shall forward the request to the appropriate agency for review. The forwarding Department organization shall include a copy of the document containing the information requested, where practicable, and its recommendation to withhold any of the information, where appropriate.

(b) Unless the agency that classified the information objects on grounds that its association with the information requires protection in the interest of national security, the Office, Board, Division or Bureau shall also notify the requester of the referral.

(c) Where the agency that classified the information objects on the grounds that its association with the information requires protection in the interest of national security, the Office, Board, Divison Bureau shall not notify the requester of the referral. After the agency that classified the information completes its review (in coordination with other agencies that have a direct interest in the subject matter) and informs the Department, a response shall be sent by the Office, Board, Division or Bureau to the requester in accordance with §17.40 or comparable procedures.

§ 17.42 Mandatory review appeal.

The Director, Office of Information and Privacy, shall establish detailed procedures that will normally enable action within 30 working days upon all appeals of denials of requests for declassification. These procedures shall provide for meaningful appellate consideration by the Department Review Committee. In accordance with these procedures, the Department shall determine whether continued classification is required in whole or in part, notify the requester of the determination, and make available any information that is a declassified and otherwise releasable. If continued classification is required under the provisions of section 3.1 of Executive Order 12356, the requester shall be notified of the reasons therefor. If requested, the Department shall also communicate the appeal of denial determination to any referring agency.

§ 17.43 Fees.

If the request requires the rendering of services for which fair and equitable fees may be charged pursuant to 31 U.S.C. 9701, such fees may be imposed at the discretion of the Office of Information and Privacy, in accordance with the schedule set forth in 28 CFR 16.9(b).

§ 17.44 Confirmation of existence of classified information.

The Department shall refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classifiable under this regulation.

§ 17.45 Material officially transferred.

In the case of classified information or material transferred by or pursuant to statute or Executive order from one department or agency to another in conjunction with a transfer of functions (as distinguished from transfers merely for the purpose of storage), the receiving department or agency shall be deemed to be the original classifying authority over such material for purposes of downgrading and declassification.

§ 17.46 Material not officially transferred.

(a) When any Office, Board, Division or Bureau of the Department has in its possession any classified information or material originated in an agency or department outside of the Department, which has since ceased to exist, and whose files and other property have not been officially transferred to another agency or department within the meaning of § 17.45, the head of the Office, Board, Division or Bureau (or his/her designee) with custodial jurisdiction over the information shall have the authority to declassify or downgrade such information. In addition, if it is impossible for the possessing Office, Board, Division or Bureau of the Department to identify the originating agency, and a review of the material indicates that the classified information contained therein should be downgraded or declassified, the head of the Office, Board, Division or Bureau concerned (or his/her designee) shall have the authority to declassify or downgrade such classified information.

(b) When it appears probable that another department or agency may have a substantial interest in whether the classification of any particular information should be maintained, the possessing Office, Board, Division or Bureau within the Department shall not exercise the declassification authority discussed in § 17.46(a), except following consultation with the other department or agency, until 60 days after the Office, Board, Division or Bureau concerned has notified, in writing, such other department or agency of the nature of the information and of its intention to downgrade or declassify the information concerned. During such a 60-day period, the other department or agency may, if it so desires, express its objections to downgrading or declassifying the particular information; however, the authority to make the ultimate decision shall reside with the head of the possessing Office, Board, Division or Bureau (or his designee).

(c) Classification guidance may be sought from appropriate officials of the Office, Board, Division or Bureau concerned, from the Department Security Officer or from the Department Review

Committee, in such instances, as described in this subpart. In cases of conflict, the Department Review Committee shall be the resolving authority.

§17.47 Information transferred for storage or retirement.

(a) Insofar as practicable, documents containing classified information shall be reviewed to determine whether or not such information can be downgraded or declassified prior to being forwarded to the Archives of the United States for permanent preservation. When such a review is complete, certification of classification review shall be entered on or affixed to the transmittal form or on the document itself by an authorized classifying or declassifying official. Appropriate markings reflecting downgrading or declassification shall also be indicated, pursuant to §17.66, on each document reviewed.

(b) Classified information transferred to the General Services Administration for accession into the archives of the United States shall be downgraded or declassified by the Archivist of the United States in accordance with Executive Order 12356, the directives of the Information Security Oversight Office, and Department guidelines pursuant to §17.36.

§17.48 Downgrading upon reconsideration.

Classified information that is not marked for automatic downgrading may be assigned a lower classification designation by the originator or by an official authorized to declassify the same information (see §17.32). Notice of downgrading shall be provided to known holders of the information to the extent practicable.

§17.49 Notification of changes to a lower classification or declassification.

(a) When documents containing classified information have been properly marked with specific dates or events for declassification, it is not necessary to issue notices of declassification to any holders. However, when a downgrading or declassification action is taken earlier than originally scheduled, the authority making such changes shall ensure prompt notification to all addressees to whom the information or material was originally transmitted. The notification shall specify the marking action to be taken, the authority therefor and the effective date. Upon receipt of notification, recipients shall effect the proper changes and shall notify addressees to whom, it turn, they have transmitted the classified information or material.

(b) Automatic declassification determinations under predecessor orders remain valid, unless extended pursuant to §17.17, and the information will be downgraded or declassified without notification to holders.

§17.50 Foreign relations series.

Heads of the Offices, Boards, Divisions and Bureaus should assist the Department of State in its preparation of the *Foreign Relations of the United States* series by facilitating access to appropriate classified material in their custody and by expediting declassification review of documents proposed for inclusion in the *Foreign Relations of the United States.*

Subpart D—Identification and Marking

§17.51 Policy.

(a) Information determined to require classification protection under the provisions of this regulation shall be so designated. These designations shall also be affixed to material other than paper documents, or the originator shall provide holders or recipients of the information with written instructions for protecting the information.

(b) Identification and markings shall not be used when the markings would reveal a confidential source or relationship not otherwise apparent in the documents.

(c) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in section 3.1(b) of Executive Order 12356.

§ 17.52 Marking documents (General).

(a) At the time of original classification, the following shall be shown on the face of originally classsified documents:

(1) One of the three classification levels defined in § 17.7;

(2) The identity of the original classification authority, unless he or she is the signer or approver of the document;

(3) The ''Department of Justice'' and the Office, Board, Division or Bureau of origin; and

(4) Either the date or event for declassification or the caveat, ''Originating Agency's Determination Required.''

(b) Should any downgrading markings or action be made or be scheduled to be taken, the date the downgrading should be shown on the face of the document.

(c) At the time of origin, paper copies of derivatively classified documents shall show on their face:

(1) The source of classification, i.e., a source document(s) or classification guide. If classification is derived from more than one source, the phrase ''multiple sources'' will be shown and the identification of each source will be maintained with the file or records copy of the document;

(2) The identity of the office within the Department originating the derivatively classified document;

(3) The overall classification of the document;

(4) The date or event for automatic declassification which shall be carried forward from the source material or classification guide. If the classification is derived from multiple sources, the latest date or event for declassification to the various source documents shall be applied to the new document.

(d) Foreign Government Information shall either retain its orginal classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) In addition to the foregoing, paper copies of classified documents shall be marked as prescribed in this subpart or in subpart F if the document contains Foreign Government Information. Such notations shall be carried forward from source documents to derivatively classified documents when appropriate.

§ 17.53 Marking the document with the identity of classifier.

(a) Identification of a classification authority shall be shown on the ''Classified by'' line prescribed under § 17.66 and shall be such that, standing alone, it is sufficient to identify a particular official, source document or classification guide.

(1) If any information in a document or material is classified as an act of original classification, the classification authority who made the determination shall be identified on the ''Classified by'' line, unless the classifier if also the signer or approver of the document.

(2) If the classification of all information in a document or material is derived from a single source (for example, a source document or classification guide), the ''Classified by'' line shall identify the source of original classification or classification guide, including its date.

(3) If the classification of information contained in a document or material is derived from more than one source document, classification guide, or combination thereof, the ''Classified by'' line shall be marked ''multiple sources'' and identification of all such sources shall be maintained with the file or record copy of the document.

(4) If an official with requisite classification authority has been designated by the head of an Office, Board, Division or Bureau to approve security classifications assigned to all information leaving that component, the name and title of that designated official shall be shown on the ''Classified by'' line. The designated official shall maintain records adequate to support derivative classification actions by other organizations.

(5) If the identification of the classifier in itself is classified information, a substitute identifier can be used provided that adequate records are maintained by the classifying organization to identify the classifier by name.

(b) Guidance concerning the identification of the classification authority on electronically transmitted messages is contained in § 17.60.

§17.54 Overall and page marking.

(a) Except as otherwise specified for working papers, the highest classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked, stamped or affixed permanently at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page shall be marked with the designation ''UNCLASSIFIED'' when appropriate.

(b) As an alternative, the highest classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page (regardless of the actual classification of the information contained on that page), provided that such marking is necessary to achieve reproduction efficiency and that the particular information in the interior pages to which classification is assigned is otherwise sufficiently identified consistent with the intent of §17.56. In no event shall the overall classification marking of a page take the place of the classification marking of portions of the page marked with lower levels of classification.

§17.55 Marking components of documents.

When major components of complex documents are likely to be used separately, each major component shall be marked as a separate document. Examples include: Each annex, appendix, or similar component of a plan or program; attachments and appendices to a memorandum or letter; and each major part of a report.

§17.56 Paragraph or portion marking.

(a) Each section, part or paragraph, of a classified document shall be marked to show the level of classification of the information contained in or revealed by it, or that it is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which portions contain or reveal classified information.

(1) Classification levels of paragraphs or portions of a document shall be shown by placing a parenthetical designator immediately preceding or following the text that it governs. In marking sections, parts, paragraphs, subparagraphs, or similar portions, the parenthetical designators ''(TS)'' for Top Secret, ''(S)'' for Secret, and ''(C)'' for Confidential, shall be used.

(2) When appropriate, the symbol ''U'' for Unclassified may be used, provided its use or nonuse is consistent throughout the document. Where required the symbols ''RD'' for Restricted Data and ''FRD'' for Formerly Restricted Data shall be added, e.g., ''(S–RD)'' or ''(C–FRD).'' In addition, portions that contain Critical Nuclear Weapon Design Information will be marked ''CNWDI'' following the classification.

(b) Illustrations, photographs, figures, graphs, drawings, charts and similar portions of classified documents will be clearly marked to show their classification or unclassified status. Such markings shall not be abbreviated and shall be prominent and placed within or contiguous to the portion. Captions of such portions shall be marked on the basis of their content alone, by placing the symbol ''(TS),'' ''(S),'' ''(C),'' or ''(U)'' immediately preceding the caption.

(c) If the application of parenthetical designation marking is determined to be impracticable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification. When all portions of a classified document are classified at the same level, this fact may be indicated by a statement to that effect, which is included in the document.

(d) When elements of information in one portion require different classifications, but segregation into separate portions would destroy continuity or context, the highest classification required for any item shall be applied to that portion or paragraph.

(e) The Attorney General may, for good cause and in writing, grant and revoke waivers of the foregoing portion marking requirements.

(1) Requests for a waiver of portion marking requirements shall be submitted to the Department Security Officer from the Security Programs Managers and shall include the following:

(i) Identification of the information or class of documents for which the waiver is sought;

(ii) A detailed explanation of why the waiver should be granted;

(iii) The written determination of the Office, Board, Division or Bureau that the anticipated dissemination of the information or class of documents for which the waiver is sought is minimal; and

(iv) The extent to which such information subject to the waiver may be a basis for derivative classification in future documents.

(2) If there is some other basis to conclude that the potential benefits of portion markings are clearly outweighed by the increased administrative burdens, a letter to the Department Security Officer from the Security Programs Manager should be submitted setting forth the circumstances.

(3) The Director of the Information Security Oversight Office shall be notified by the Department Security Officer of any waivers.

§ 17.57 Subjects and titles of documents.

Subjects or titles of classified documents must be marked with the appropriate symbol, ''(TS),'' ''(S),'' ''(C),'' or ''(U)'' and shall be placed immediately to the right of such subjects or titles. When applicable, other appropriate symbols, e.g., ''(RD)'' and ''(FRD),'' shall be added. Every effort should be made to use unclassified titles or subjects. However, if a title or subject requires classification, an unclassified identifier may be assigned to facilitate reference.

§ 17.58 Files, folders or groups of documents.

Files, folders or groups of documents shall be marked conspicuously according to the highest classification of any classified document included therein. Document cover sheets may be used for this purpose.

§ 17.59 Transmittal documents.

A transmittal document shall carry on its face a prominent notation as to the highest classification of the information transmitted with it and a legend showing the classification, if any, of the transmittal document standing alone. For example, an unclassified document that transmits a classified document shall bear a notation substantially as follows: ''UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS REMOVED.''

§ 17.60 Messages.

It is recognized that marking some electronically transmitted classified messages poses serious technical problems, requiring certain exceptions. However, every reasonable effort shall be made to mark such messages consistent with the provisions of this subpart. Message abbreviations examples are included in § 17.66.

§ 17.61 Translations.

Translations of U.S. classified information into a language other than English shall be marked to show the United States as the country of origin, with the appropriate U.S. classification markings and the foreign language equivalent.

§ 17.62 Markings on special categories of material.

(a) Security classification and declassification instructions assigned by the classifier shall be consistent with § 17.51. In addition to use of a stamped marking, classification levels may be printed, written, painted, or affixed by means of a tag, sticker, decal or similar device, on classified material other than paper copies of documents, with preference given to the most durable.

(b) If marking the material or container is not practicable, written notification of the security classification and declassification instructions shall be furnished to recipients. The following procedures for marking various kinds of material containing classified information are not all inclusive and may be varied to accommodate the physical characteristics of the material containing the classified information as well as organizational and operational requirements.

§ 17.63 Charts, maps and drawings.

Charts, maps and drawings shall bear the appropriate classification marking under the legend, title block or scale,

in a manner that differentiates between the overall classification of the document and the classification of the legend or title itself. The higher of these markings shall be inscribed at the top and bottom of each such document. If folding or rolling charts, maps or drawings would obscure the classification markings, additional markings shall be applied that are clearly visible when the document is folded or rolled.

§17.64 Photographs, films and recordings.

Photographs, films (including negatives), recordings, and their containers shall be marked in such a manner as to assure that a recipient or viewer will know that classified information of a specified level of classification is involved.

§17.65 Applying derivative declassification markings.

New material that derives its classification from existing classified material shall be treated as follows:

(a) If the source material bears a declassification date or event, the date or event shall be carried forward to the new material.

(b) If the source material has no declassification date or event, or bears an indeterminate date or wording such as ''Upon Notification by Originator,'' ''Cannot Be Determined,'' ''Impossible to Determine,'' or ''Date of Review,'' the new material shall be marked ''Originating Agency's Determination Required.''

§17.66 Examples of commonly used markings.

(a) *Original classification.* At the time of origin, each classified document is marked on its face with one or more standard markings substantially as shown below in addition to other markings contained in §17.52.

(1) The following markings are used with an original classification when there is a specific event or date for declassification:

CLASSIFIED BY: (Classification Authority)
DECLASSIFY ON: (Date or Event)
and Message Abbreviation: DECL (Date or Event)

(2) The following markings are used with an original classification when a date or event for declassification cannot be determined:

CLASSIFIED BY: (Classification Authority)
DECLASSIFY ON: Originating Agency Determination Required or (OADR)
and Message Abbreviation: DECL (OADR)

(b) *Downgrading and Declassification.* Declassification and, as applicable, downgrading instructions shall be shown as follows:

(1) For information to be declassification automatically on a specific date:

DECLASSIFY ON: (Date)
and Message Abbreviation: DECL: (Date)

(2) For information to be declassified automatically upon occurrence of a specific event:

DECLASSIFY ON: (Description of Event)
and Message Abbreviation: DECL: (Description of Event)

(3) For information not to be declassified automatically:

DECLASSIFY ON: Originating Agency's Determination Required or OADR
and Message Abbreviation: DECL: OADR

(4) For information to be downgraded automatically on a specific date or upon occurrence of a specific event:

DOWNGRADE TO (Classification Level)
ON (Date or Description of Event)
and Message Abbreviation:
DNG (abbreviation of classification level to which the information is to be downgraded and date or description of event on which downgrading is to occur)

(c) *Derivative classification.* Documents classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in §§17.51 through 17.66 as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide.

(1) The authority for derivative classification shall be shown as follows:

CLASSIFIED BY: (Description of source document or classification guide)
and a Message Abbreviation is not required.

(i) If a document is classified on the basic of more than one source document or classification guide, the authority for classification shall be shown as follows:

CLASSIFIED BY MULTIPLE SOURCES

In these cases, the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document.

(ii) A document derivatively classified on the basis of a source document that is marked ''CLASSIFIED BY MULTIPLE SOURCES'' shall cite the source document in its ''CLASSIFIED BY'' line rather than the term ''MULTIPLE SOURCES.''

(2) Dates or events for automatic declassification or downgrading, or the notation ''ORIGINATING AGENCY'S DETERMINATION REQUIRED'' to indicate that the document is not to be declassified automatically, shall be carried forward from the source document, or as directed by a classification guide, and shown on a ''DECLASSIFY ON'' line as follows:

DECLASSIFY ON: (Date, Description of Event, or Originating Agency's Determination Required or OADR)
and Message Abbreviation: DECL (Date, Description of Event, or OADR)

(d) *Restricted Data.* The Restricted Data and Formerly Restricted Data markings are, in themselves, evidence of extended classification. Therefore, except for electronically transmitted messages, only a completed ''Classified By'' line is required with such a marking.

(1) Classified documents or material containing Restricted Data as defined in the Atomtic Energy Act of 1954, as amended, shall be marked as follows on the bottom of each page:

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

(2) Classified documents or material containing Formerly Restricted Data, as defined in the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2162(d), but no Restricted Data, shall be marked as follows on the bottom of each page:

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination, Atomic Energy Act of 1954, as amended, 42 U.S.C. 2164(b).''

(e) *Intelligence sources or methods information.* Classified information or material involving intelligence sources or methods that is subject to specific dissemination controls shall be marked with the following additional warning notice, unless otherwise proscribed by the Director of Central Intelligence.

WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED.
The message abbreviation WNINTEL shall be used on applicable electrically transmitted messages unless proscribed by the Director of Central Intelligence.

(f) *Foreign Government Information.* Documents that contain Foreign Government Information shall include either the marking ''FOREIGN GOVERNMENT INFORMATION,'' or a marking that otherwise indicates that the information is Foreign Government Information. When Foreign Government Information must be concealed, the document shall be marked as if it were wholly of United States origin. The message abbreviation FGI shall be used on applicable electrically transmitted messages unless the fact that the information is of foreign origin must be concealed.

§ 17.67 Upgrading.

When material is upgraded it shall be promptly and conspicuously marked, except that in all such cases the old classification markings shall be cancelled and new markings substituted therefor. All upgrading shall be in accordance with § 17.28.

§ 17.68 Limited use of posted notice for large quantities of material.

(a) When the volume of material is such that prompt remarking of each classified item cannot be accomplished without unduly interfering with operations, the custodian may attach upgrading, downgrading or declassification notices to the storage unit. Each notice shall specify the authority for the classification action, the date of the action, and the storage unit to which it applies.

(b) When individual documents or materials are permanently withdrawn from storage units, they shall be remarked promptly. However, if documents or materials subject to a downgrading or declassification notice are

withdrawn from one storage unit solely for transfer to another, or a storage unit containing such documents or materials is transferred from one place to another, the transfer may be made without remarking, provided that in all instances the notice is attached to or remains with each shipment. Items permanently withdrawn from such storage units shall be promptly remarked in accordance with this subpart.

§17.69 Additional warning notices.

Should the marking requirements prescribed in §17.52 not be adequate, additional warning notices shall be prominently displayed on classified documents or materials, as applicable. In the case of documents, these warning notices shall be marked conspicuously on the outside of the front cover, or on the first page, if there is no front cover.

§17.70 Dissemination and reproduction notice.

Classified information that is determined by a Department originator to be subject to special dissemination or reproduction limitations, or both, shall include an appropriate statement(s) on its cover sheet or the first page of the text, substantially as follows:

''Reproduction requires approval of originator or higher Department of Justice Authority.''

''Further dissemination only as directed by (Insert appropriate office or official) or higher Department of Justice authority.'' or ''Eyes Only.''

Subpart E—Safekeeping and Storage

§17.71 Policy.

(a) Classified information may be used, discussed, held, or stored only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it. The exact nature of security requirements will depend on a thorough security evaluation of local conditions and circumstances. Security requirements must permit the accomplishment of essential functions while affording selected items of information reasonable degrees of security with a minimum of risk. The requirements specified in this regulation represent the minimum acceptable standards.

(b) Funds, weapons, medical items, or other items of intrinsic value will not be stored in containers with classified National Security Information. This restriction does not apply to valuable items which are themselves classified.

§17.72 Standards for storage equipment.

The General Services Administration establishes and publishes minimum uniform standards, specifications, and supply schedules for containers, vaults, alarm systems and associated security devices suitable for storage and protection of classified information and material throughout the Government. Department Order 2620.4 entitled, ''Physical Security Manual for Safeguarding Classified National Security Information'' contains information regarding acceptable security equipment for the physical protection of National Security Information within the Department. No other equipment to be used for the storage of classified National Security Information shall be procured without the prior approval of the Department Security Officer.

§17.73 Storage of classified material.

Classified material, including classified information stored on removable storage media used by typewriters, word processors or remote terminal equipment, must be protected at all times. Whenever classified material is not under the personal control of an authorized and appropriately cleared person, whether during or outside of working hours, it will be guarded or stored in a locked security container as prescribed below:

(a) *Top Secret*. Top Secret information or material shall be stored in:

(1) A safe-type steel file container having a built-in, three-position, dial-type changeable combination lock appoved by the General Services Administration or a vault or secure area which meets the standards as contained in the Subject Manual cross referenced in Department Order 2620.4, or

(2) An alarmed area, provided such facilities are judged by the Department Security Officer to afford protection

equal to or greater than that prescribed in paragraph (a)(1) of this section. When an alarmed area is utilized for the storage of Top Secret information and material, the physical barrier must be adequate to prevent surreptitious removal or observation of the material. The physical barrier must also be such that attempted forcible entry will give evidence of such entry into the area or room. As a minimum the alarm system must provide for an immediate response by a security force to an attempted surreptitious or forced entry.

(b) *Secret and Confidential.* Secret and Confidential material may be stored in a manner authorized for Top Secret; or in a vault-type room, or secure storage room which has been approved in accordance with the standards prescribed in the Subject Manual cross referenced in Department Order 2620.4, or until phased out, in containers described in paragraph (d) of this section.

(c) *Specialized security equipment*—(1) *One and two-drawer containers.* One and two-drawer security containers which are approved by the General Services Administration shall be used primarily in mobile facilities or in areas where small amounts of classified information are stored. Such containers should be securely fastened or guarded to prevent the theft of the container.

(2) *Map and plan file.* A General Services Administration approved Map and Plan File container has been developed for storage of odd-sized items such as computer cards and tapes, maps, charts, plans, and other classified material.

(d) *Non-General Services Administration approved containers.* In addition to the security containers meeting General Services Administration standards, Secret and Confidential classified information may be stored in a steel filing cabinet equipped with a built-in, three-position, dial-type changeable combination lock; or as a last resort, in an existent steel filing cabinet equipped with a steel lock bar, provided it is secured by a General Services Administration approved changeable combination padlock. If a steel filing cabinet with a steel lock bar is used for Secret information, the procedures in Department Order 2620.4 must be adhered to.

(e) *Sensitive Compartmented Information storage.* Sensitive Compartmented Information will be stored only in accredited facilities which meet approved physical security standards for such material pursuant to Director of Central Intelligence Directive 1/19 entitled, ''Uniform Procedures for Administrative Handling and Accountability of Sensitive Compartmented Information'' and other applicable Department regulations. When maintained in Sensitive Compartmented Information facilities, classified information may be stored in the same container prescribed for storage of Sensitive Compartmented Information; however, when removed from the Sensitive Compartmented Information facility, the provisions of §17.73 (a) through (d) above apply.

§ 17.74 Procurement and phase-in of new storage equipment.

Whenever new security storage equipment is procured, it will be from the security containers listed on the Federal Supply Schedule, General Services Administration.

(a) Further acquisition for unapproved security containers or modification of cabinets to bar-padlock type as storage equipment for classified information and material is prohibited. Exceptions may be made by the Department Security Officer, upon written request from the Security Programs Manager concerned.

(b) When a security storage container is acquired, the Security Programs Manager shall ensure that a new combination is set before the container is put into use.

§ 17.75 Designations of security containers.

There shall be no external marking as to the level of classified information authorized to be stored in a container. However, each vault, secure area or security container shall be assigned a number or symbol for the purpose of identifying what level or category of clasified information is stored therein. The number or symbol shall be affixed in a conspicuous location on the outside of the vault or security container. Security Programs Managers shall

keep a record of the vaults and security containers under their cognizance along with the designation of the level of classified information authorized to be stored therein.

§ 17.76 Changing combinations to security containers.

Combinations to security containers and dial-type locks will be changed only by individuals having an appropriate security clearance and who have received instruction on how to correctly change such combinations. Combinations shall be changed:

(a) When the container is placed in use;

(b) When an individual knowing the combination no longer requires or is authorized access to classified information stored in the container;

(c) When the combination or record of combination has been subject to compromise;

(d) When taken out of service; or

(e) At least annually.

§ 17.77 Equipment out of service.

When security storage equipment is taken out of service, it shall be inspected to ensure that no classified information remains.

(a) Security Programs Managers shall establish procedures to certify that whenever security equipment is moved or relocated or ''out of service'' or ''excess'' that the security equipment does not contain classified information.

(b) When taken out of service, built-in combination locks shall be reset to the standard combination 50–25–50. Combination padlocks shall be reset to the standard combination 10–20–30.

§ 17.78 Classification of combinations.

The combination of a vault or container used for the storage of classified information and material shall be assigned a security classification no lower than the highest level of the classified material authorized to be stored therein. No downgrading/declassification instructions or classifier identity are required to be made when classifying records of combinations to security containers. Accordingly, classification actions for such combinations are not required to be reported. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes.

§ 17.79 Recording storage facility data.

A record shall be maintained by Security Programs Managers or their designees for each vault, secure area, or container used for the storage of classified information. The record shall show its location, and the names and other appropriate identifying data of persons having knowledge of the combinations to such storage facilities. General Services Administration Optional Form 63, entitled, ''Security Container Information'' may be used within the Department for these purposes. The OF–63 containing security combinations shall be marked with the appropriate overall classification, and shall be safeguarded and stored in accordance with the protection afforded to that classification.

§ 17.80 Care during working hours.

Each individual shall take all necessary precautions to prevent access to classified information by unauthorized persons (i.e., persons who do not possess an appropriate security clearance, and who do not possess the required need-to-know). Among the precautions to be followed are:

(a) Classified documents, when removed from storage for working purposes, shall be kept under constant surveillance and turned face-down or covered when not in use. Department Cover Sheets should be utilized to cover classified documents.

(b) Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information shall be either destroyed by the person responsible for their preparation immediately after they have served their purposes, or shall be given the same classification and safeguarded in the same manner as the classified information they contain.

(c) Classified information handled by word processors or remote terminals is susceptible to interception by unauthorized persons due to unintended electrical emanations. Word processors or remote terminals used frequently to handle classified information must

have a reduced level of emanations (e.g., approved by the Subcommittee on Compromising Emanations) or located in an area with a sufficient perimeter of control.

(d) Typewriter ribbons used in typing classified information shall be protected in the same manner as the highest level of classification for which they have been so used. When destruction is necessary, it shall be accomplished in the manner prescribed for classified working papers (See subpart H) of the same classification. After the upper and lower sections of the ribbon have been cycled through the typewriter five times in the course of regular typing, all fabric ribbons may be treated as unclassified. Carbon and plastic typewriter ribbons and carbon paper which have been used in the production of classified information shall be destroyed after initial usage in the manner prescribed for working papers of the same classification. As an exception to the foregoing, any typewriter ribbon which remains substantially stationary in the typewriter after it has received at least five consecutive impressions may be treated as unclassified.

§ 17.81 Care after working hours.

Heads of Offices, Boards, Divisions and Bureaus shall require and institute through their Security Programs Managers, a system of security checks at the close of each working day to ensure that the classified information in the possession of such Offices, Boards, Divisions and Bureaus is properly protected. Security Programs Managers shall require the custodians of classified information in their Offices, Boards, Divisions or Bureaus to make periodic inspections of their respective areas which shall ensure that the following minimum requirements are met:

(a) All classified information is stored in approved security containers. This includes removable storage media, e.g., floppy disks used by word processors, that contain classified information.

(b) Burn bags, if utilized, are either stored in approved security containers or destroyed.

(c) Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts and similar papers have been properly stored or destroyed.

§ 17.82 Administrative aids for safeguarding classified material.

Appropriate forms shall be used on security containers for check purposes. Such forms shall be conspicuously attached to the outside of each container used for the storage of classified information. Each authorized person will record the time and date that he or she unlocks or locks the security container, followed by the person's initials. At the close of each working day, a person other than the individual locking the container will check the container, in the presence of the individual locking the container, to ensure that it is secure. The time of the check followed by the checker's initials will be recorded. The check will be conducted each working day. If a container has not been opened, the date and the phrase ''Not Opened'' will be noted in addition to the time and the checker's initials. A container will not be left unattended until it has been locked by an authorized person and checked by a second person. The person locking a container is responsible for insuring that another person checks the container. Reversible ''OPEN-CLOSED'' signs, shall be utilized on security containers containing classified information. The respective side of the sign shall be displayed to indicate when the container is open or closed.

§ 17.83 Telephone or telecommunication conversations.

(a) Classified information shall not be discussed over nonsecure telephones. Classified telephone conversations are authorized only over approved secure (encrypted) communication circuits. Information concerning which telephones in the Department are secure may be obtained from Security Programs Managers or the Department Security Officer.

(b) Classified information shall not be transmitted over nonsecure radio equipment or facsimile devices. Classified information may be transmitted

using approved secure (encrypted) communication equipment. Guidance on which communication equipment is secure may be obtained from the Security Programs Manager or the Department Security Officer.

§17.84 Security of meetings and conferences.

The official responsible for arranging or convening a conference or other meeting is also responsible for instituting procedures and selecting facilities which provide adequate security if classified information is to be discussed or disclosed. (See Department Order 2660.1A.) The responsible official will:

(a) Notify each person who is to be present or who is to discuss classified information or any security limitations that must be imposed because of:

(1) The level of access authorization.

(2) Requirement for access to the information by the attendees.

(3) Physical security conditions.

(b) Ensure that each person attending the classified portions of meetings has been authorized access to information of equal or higher classifiation than the information to be disclosed.

(c) Ensure that the area in which classified information is to be discussed affords adequate acoustical security against unauthorized disclosure.

(d) Ensure that adequate storage facilities are available, if needed.

(e) Control and safeguard any classified information furnished to those in attendance and retrieve the material or obtain receipts, as required.

(f) Monitor the meetings to ensure that discussions are limited to the level authorized.

(g) Ensure that meetings at which classified information is to be discussed will be held only in a U.S. Government area or at a cleared facility of a Department contractor or consultant. When necessary for the accomplishment of essential functions, a meeting involving classified information may be held at another location provided it has been specifically authorized by the Department Security Officer.

Subpart F—Foreign Government Information

§17.85 Identification of documents.

Foreign Government Information under this regulation is of two types and shall be classified in accordance with this subpart.

(a) Information, whether classified or unclassified, provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, express or implied, that the information, the source of the information, or both, are to be held in confidence shall be classified by the Office, Board, Division, or Bureau receiving the document.

(b) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence shall be classified.

§17.86 Classification.

(a) Foreign Government Information classified and provided by a foreign government or international organization of governments shall retain its original classification designation or be assigned a United States classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

(b) Foreign Government Information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that it be held in confidence must be classified. Therefore, such Foreign Government Information shall be classified at least Confidential, and higher whenever the damage criteria for Secret and Top Secret in subpart B are determined to be met.

§17.87 Presumption of damage by unauthorized disclosure.

Unauthorized disclosure of Foreign Government Information, the identity

of a confidential foreign source or intelligence sources or methods is presumed to cause damage to the national security.

§ 17.88 Duration of classification.

(a) Foreign Government Information marked for automatic declassification shall be declassified unless extended by an authorized official of the originating agency.

(b) Unless classification guidelines developed pursuant to subpart B prescribed dates or events for declassification, Foreign Government Information may be classified by the Department as required by national security considerations.

§ 17.89 Systematic review.

(a) The Attorney General may, in consultation with the Archivist of the United States and, where appropriate, with the foreign governments or international organizations concerned, develop systematic review guidelines for 30-year old Foreign Government Information in the possession or under the control of the Department. These guidelines shall be kept current through review by the Attorney General at least once every five years unless earlier review for revision is requested by the Archivist of the United States.

(b) The Director, Office of Information and Privacy, shall perform administrative functions necessary to effect such review by the Attorney General.

(c) These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the Attorney General, be used by any agency having custody of the same categories of information.

§ 17.90 Mandatory review.

(a) Requests for mandatory review for declassification of Foreign Government Information shall be processed and acted upon in accordance with the provisions of §§ 17.37 through 17.46, except that Foreign Government Information will be declassified only in accordance with the classification guidelines developed for such purpose and after necessary consultation with other Government agencies with subject matter interest.

(b) In cases where the above guidelines cannot be applied to the Foreign Government Information requested, or in the absence of such guidelines, consultation with the foreign originator through appropriate channels should be effected prior to final action on the request. When the responsible Office, Board, Division or Bureau is knowledgeable of the foreign originator's view toward declassification or continued classification of the types of information requested, consultation with the foreign orginator may not be necessary.

(c) If the Office, Board, Division or Bureau receiving the mandatory review request did not receive or classify the Foreign Government Information, it shall refer the request to the appropriate agency for action. The agency that initially received or classified the Foreign Government Information shall be responsible for making a declassification determination after consultation with other concerned agencies.

§ 17.91 Equivalent United States classification designations.

Except for the foreign security classification designation ''restricted,'' foreign classification designations, including those of international organizations of governments, i.e., NATO and CENTO, generally parallel United States classification designations.

§ 17.92 Marking other foreign government documents.

(a) If the security classification designation of foreign government documents is shown in English, no other classification marking shall be applied. If the security classification designation is not shown in English, the equivalent overall U.S. classification designation shall be marked conspicuously on the document. In those cases where foreign government documents are marked with a classification designation having no U.S. equivalent, such documents shall be marked and handled in accordance with § 17.92(b).

(b) Certain foreign governments and international organizations of governments use a fourth classification designation below Confidential. Such classification is frequently designated as

''Restricted'' by such entities. If foreign government documents are marked with such a classification designation, whether or not in English, the U.S. classification marking Confidential shall be applied and the Foreign Government Information so designated shall be protected as U.S. Confidential information.

(c) Dates for declassification or for review for declassification shall be marked on foreign government documents only as required by §§17.88 and 17.89.

(d) In most cases, other marking requirements prescribed by this regulation for U.S. classified documents are not applicable to documents of foreign governments or international organizations of governments.

§17.93 Marking of Foreign Government Information in Department documents.

(a) When Department documents contain Foreign Government Information, the marking ''FOREIGN GOVERNMENT INFORMATION'' or a marking that otherwise indicates that the information is Foreign Government Information shall be shown on the face of the document.

(b) Where such markings would reveal Foreign Government Information incorporated into Department documents that must be concealed as to its source, the markings shall not be used.

(c) The requirement for portion markings may be satisfied by including the appropriate identification in the portion or paragraph classification markings, e.g., (NATO–S) or (U.K.–C).

§17.94 Other Foreign Government Information.

Classified Foreign Government Information held by an Office, Board, Division or Bureau shall be safeguarded or protected as prescribed by this regulation for United States classified information of a comparable level.

Subpart G—Access, Dissemination, and Accountability

§17.95 Policy.

(a) No person may be given access to classified information or material originated by, in the custody or under the control of the Department, unless that person has been determined to be trustworthy and (except as provided in §17.96(e)) unless access is necessary for the performance of official duties. Procedures shall be established by the Security Program Managers of the Offices, Boards, Divisions and Bureaus to prevent any unnecessary access to classified information. No person is authorized to have access to classified information solely by virtue of rank or position. Accordingly, all requests from the heads of the Offices, Boards, Divisions and Bureaus to the Department Security Officer for a personnel security clearance shall contain a demonstrable need for access to classified information. Further, the number of persons cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs.

(b) The determination of trustworthiness for eligibility for access to classified information (referred to as a security clearance) shall be made by the Department Security Officer or his designee and shall be based on appropriate security background investigations in accordance with applicable Executive Orders, Department regulations, Intelligence Community directives and Office of Personnel Management guidelines. Current and valid clearances issued to persons by other agencies of the Executive Branch may be accepted, for access purposes only, in lieu of granting such clearances by the Department Security Officer. Such clearance certification shall be accomplished by the Department Security Officer, upon request.

(c) The Department Security Officer may delegate, in writing, the authority to grant Department employees security clearances to qualified Security Programs Managers when the operational need justifies such delegation and the Department Security Officer is assured that such officials shall continually apply all clearance criteria in a uniform and correct manner during the adjudication of personnel security investigations. In those instances where such authority is delegated, the Department Security Officer shall reserve

the right to review all personnel security cases which contain derogatory information that could be a deterrent to eligibility for clearance. The Department Security Officer shall reserve the right to withdraw such authority in any instance where it is determined that Department clearance policy and criteria set forth herein are not being expressly followed.

§ 17.96 Access by persons outside the Executive Branch.

Classified information shall not be disseminated outside the Executive Branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the Executive Branch.

(a) *General.* In accordance with the provisions of Department Order 2620.6, classified information originated by, or in the custody of, the Department may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Government will derive a benefit or advantage, and that such release is approved by the Attorney General or the Assistant Attorney General for Administration, and is not prohibited by the originating department or agency (or foreign government in the case of Foreign Government Information). Recipients must be shown to be trustworthy by the Department Security Officer and recipients must agree to safeguard the information in accordance with the provisions of this regulation. Heads of Offices, Boards, Divisions and Bureaus shall determine, prior to the release of classified information, the propriety of such action, in the interest of the national security and the recipient's security clearance status and need-to-know.

(b) *Congress.* Access to classified information by Congress, its committees, members, and staff representatives shall be in accordance with the provisions of Department Order 2620.6. Any Department employee testifying before a Congressional Committee in executive session in relation to a classified matter shall obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of the information that may be discussed. Members of Congress, by virtue of their elected positions, are not investigated or cleared by the Department.

(c) *Non-contractor personnel.* Personnel outside the Executive Branch who are not subject to any Department contracts or grants and therefore are exempt from the provisions of the Defense Industrial Security Program and who require access to classified information originated by or in the custody of the Department shall be processed for such clearance in accordance with the provisions of Department Order 2620.6.

(d) *Contractor personnel.* Personnel who are subject to a Department contract or grant or who are rendering consultant services to the Department and require access to classified information originated by or in the custody of the Department shall be processed for such access/clearance in accordance with the provisions of the Defense Industrial Security Program and Department Order 2600.3A.

(e) *Historical researchers and former Presidential appointees.* (1) The requirement in §17.95 that access to classified information may be granted only as is necessary for the performance of official duties may be waived for persons who:

(i) Are engaged in historical research projects or

(ii) Have previously occupied policy-making positions to which they were appointed by the President.

(2) All persons receiving access pursuant to this subparagraph must have been determined to be trustworthy by the Department Security Officer as a precondition before receiving access. such determination shall be based on such investigation as the Department Security Officer deems appropriate. Historical researchers and former Presidential appointees shall not have access to Foreign Government Information without the written permission from appropriate authority of the foreign government concerned.

(3) Waivers of the ''need-to-know'' requirement under this paragraph may be granted by the Department Security Officer provided that the Security Programs Manager of the Office, Board, Division or Bureau with classification

jurisdiction over the information being sought;

(i) Makes a written determination that such access is consistent with the interests of national security;

(ii) Limits such access to specific categories of information over which the Department has classification jurisdiction;

(iii) Maintains custody of the classified information at a Department facility; and

(iv) Obtains the recipient's written and signed agreement to safeguard the information in accordance with the provisions of this regulation and to authorize a review of any notes and manuscript for determination that no classified information is contained therein;

(v) And in the case of former Presidential appointees, limits their access to items that such former appointees originated, reviewed, signed or received while serving as a Presidential appointee and ensures that such appointee does not remove or cause to be removed any classified information reviewed.

(4) If access requested by historical researchers and former Presidential appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to 31 U.S.C. 9701, the requester shall be so notified and fees may be imposed.

(f) *Access by persons within the Judicial Branch.* To have access to classified information, every person except for Federal judges appointed by the President, including but not limited to court reporters, typists and secretaries, law clerks and translators must be granted the appropriate clearance by the Department Security Officer. Before clearance can be granted to any individual outside the Executive Branch who requires access to classified information originated by or in the custody of the Department, the person must have a complete and current full-field background investigation to allow a determination of eligibility for a security clearance to be made. This full-field investigation is conducted by the Federal Bureau of Investigation or the Office of Personnel Management. The length of time it generally takes to complete an expedited full-field background investigation is 90 days. Therefore, the courts should be advised of the time required to satisfy Executive Branch security regulations. All persons requiring access to classified information should be identified as promptly as possible by the Department's legal counsel to ensure the earliest possible beginning of clearance procedures.

(g) *Judicial proceedings.* (1) Any Department employee or organization receiving an order or subpoena from a Federal or State court to produce National Security Information, required to submit National Security Information for official Department litigative purposes, or receiving National Security Information from another organization for production of such in litigation, shall immediately determine from the agency originating the classified information whether the information can be declassified.

(2) If declassification is not possible, the Department employee or organization and the assigned Department legal counsel in the case shall take all appropriate action to protect such information pursuant to the provisions of this paragraph.

(3) If a determination is made to produce such information in a judicial proceeding in any manner, the assigned Department legal counsel shall take all steps necessary to ensure the cooperation of the court and where appropriate, opposing counsel, in safeguarding and retrieving the information pursuant to the provisions of this regulation.

(4) The Classified Information Procedures Act, Public Law 96–456, 94 Stat. 2025, 18 U.S.C. App. (Supp. 1983), and the ''Security Procedures Established Pursuant to Public Law 96–456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information,'' may be used in Federal criminal cases involving classified information. In judicial proceedings other than Federal criminal cases or where the Classified Information Procedures Act is not used, the following minimum security safeguards shall be requested of the court and, where appropriate, sought to be included in a judicial protective order:

(i) Every effort shall be made to limit production of classified information to an *in camera, ex parte* review by the court to determine the relevance of the classified information in question.

(ii) Classified information shall not be introduced into evidence or otherwise disclosed at a proceeding without the prior approval of either the originating agency, the Attorney General, or the President.

(iii) Attendance at any proceeding where classified information is to be introduced or disclosed should be limited to the judge(s) as defined in Department Order 2620.6 and to those other persons whose duties require knowledge or possession of the classified information who have been determined to be trustworthy by the Department Security Officer.

(iv) All such proceedings shall be held in a court facility which can provide appropriate protection for the classified information as determined by the Department Security Officer.

(v) Dissemination and accountability controls shall be established for all classified information offered for indentification or introduced into evidence at such proceedings.

(vi) All transcripts of such proceedings shall be appropriately marked to show the classified portions and placed under seal upon transcription.

(vii) All classified information including the appropriate portions of the transcript shall be handled and stored in a manner consistent with the provisions of this regulation.

(viii) At the conclusion of the proceeding, all classified information shall be returned to the Department or placed under seal by the court.

(ix) All classified notes, drafts, or any other documents generated during the course of the proceedings and containing classified information shall be retrieved by Department employees and immediately transferred to the Department for safeguarding and destruction as appropriate.

(x) All persons who become privy to classified information disclosed under the provisions of this section shall be fully advised as to the classification level of such information, all pertinent safeguarding and storage requirements, and their liability in the event of unauthorized disclosure.

(xi) The Department Security Officer, in consultation with the agency originating classified case-related information and Government attorneys, may waive any of the security requirements identified in paragraph (g)(4)(iii)—(x) of this section, if it has been determined that such a waiver is in the interest of the national security.

(5) This paragraph shall apply to all litigation, including matters arising under the Freedom of Information Act, 5 U.S.C. 552, as amended.

§ 17.97 Access by foreign nationals, foreign governments, international organizations, and immigrant aliens.

(a) Classified information may be released to foreign nationals, foreign governments and international organizations only when authorized under the provisions of the National Disclosure Policy (NDP–1) issued by the Secretary of Defense.

(b) If it is in the interest of the national security, Secret and Confidential information may be released, on a limited basis, to immigrant aliens in the performance of official duties, provided that the Department Security Officer determines the individual is reliable and trustworthy in accordance with this subpart.

(c) Immigrant aliens may be granted a Limited Access Authorization to Top Secret information provided that the head of the Office, Board, Division of Bureau concerned makes a personal written request and determination to the Department Security Officer that such access is essential to meet Government requirements and that the Department Security Officer determines that the individual is reliable and trustworthy in accordance with this subpart.

§ 17.98 Procedures for requesting a security clearance for a Department employee.

Requests for determination of eligibility for a security clearance shall be in the form of a memorandum addressed from the head of the Office, Board, Division or Bureau concerned to the Department Security Officer. Exception to this requirement may be

granted in accordance with the provisions of §17.95(c). Two copies of the request shall be submitted. The memorandum shall contain the following items:

(a) *Degree of clearance requested.* National security clearances are categorized into three levels, namely, Top Secret, Secret, and Confidential. The categories of security clearances are related directly to the levels of National Security Information to which access is required.

(b) *Justification for requested clearance.* A person must have a need for access to the particular classified information or material sought in connection with his/her official duties or obligations. This need-to-know is the essence for any justification for a security clearance. The justification for a clearance does not have to be long or detailed; however, a strict need-to-know shall be established before consideration to grant a security clearance can be given.

(c) *Continuous evaluation of need-to-know.* A continuing review of the established need-to-know shall be conducted by the Security Programs Manager.

(d) *Request for administrative withdrawal.* The head of each Office, Board, Division or Bureau shall make provision to request the administrative withdrawal of a security clearance of persons for whom there is no foreseeable need for access to classified information or material in connection with the performance of their official duties; for example, termination of employment or change in position. Likewise, when a person no longer needs access to classified material bearing a particular security classification category, a request that the security clearance be adjusted to the classification category still required for the performance of his/her official duties and obligations shall be made by the Security Programs Manager of the Office, Board, Division or Bureau concerned. In both instances, such action resultant from these requests will be without prejudice to the person's eligibility for future security clearances.

§17.99 Other access situations.

When necessary in the interests of national security, the Attorney General or the Assistant Attorney General for Administration may authorize access by persons outside the Federal Government, other than those enumerated above, to classified information upon determining that (a) the recipient is trustworthy for the purpose of accomplishing a national security objective and (b) that the recipient can and will safeguard the information from unauthorized disclosure. The clearance procedures and provisions of Department Order 2620.6 shall be followed in such instances.

§17.100 Dissemination.

(a) *Policy.* Except as otherwise provided in section 102 of the National Security Act of 1947, 50 U.S.C. 403, and 17.96(f) of this regulation, classified information originating within the Department may not be disseminated outside any other agency to which it has been made available without the consent of the Department. Conversely, classified information originating in a department or agency other than the Department shall not be disseminated outside the Department without first obtaining the consent of the originating department or agency. Office, Board, Division and Bureau Security Programs Managers shall establish procedures consistent with this regulation for the dissemination of classified information. The originating official or Office, Board, Division or Bureau may prescribe specific restrictions on dissemination of classified information when necessary.

(b) *Restraint on reproduction.* No documents or materials or any portions thereof that contain Top Secret information shall be reproduced without the consent of the originator or higher authority. Any stated prohibition or markings on any classified document (regardless of classification) against reproduction shall be strictly observed. (See §17.70.) The folowing measures apply to reproduction equipment and to the reproduction of classified information:

(1) Copying of documents containing classified information shall be minimized;

(2) Officials within each Office, Board, Division or Bureau shall be authorized by the Security Programs

Manager, in writing, to approve the reproduction of Top Secret and Secret information; shall be designated by position title, and shall review the need for reproduction of classified documents with a view toward minimizing reproduction;

(3) Specific reproduction equipment shall be designated for the reproduction of classified information. Rules for reproduction of classified information shall be posted on or near the designated equipment;

(4) Notices prohibiting reproduction of classified information shall be posted on equipment used only for the reproduction of unclassified information;

(5) Security Programs Managers shall ensure that equipment used for reproduction of classified material does not leave latent images in the equipment or on other material;

(6) All copies of classified documents reproduced for any purpose, including those incorporated into a working paper, are subject to the same controls prescribed for the document from which the reproduction is made; and

(7) Records shall be maintained to show the number and distribution of reproduced copies of all Top Secret documents and of all classified documents covered by special access programs distributed outside the Department. Also, records shall be maintained concerning all Secret and Confidential documents which are marked with special dissemination and reproduction limitations.

§ 17.101 Transmission of Top Secret information.

Transmission of Top Secret information shall be effected only by:

(a) Authorized and cleared Department messenger-courier services;

(b) The Department of State Courier System;

(c) The Armed Forces Courier Service;

(d) Cleared and designated Department employee traveling on a conveyance owned, controlled or chartered by the Government;

(e) Cleared and designated Department employees traveling by surface transportation;

(f) Cleared and designated Department employees traveling on scheduled commercial passenger aircraft within and between the United States, its Territories and Canada;

(g) Cleared and designated Department contractors traveling within and between the United States and its Territories provided that the transmission has been authorized in writing by the appropriate contracting officer or his/her designated representative and, the designated employees have been briefed in their responsibilities as couriers or escorts for the protection of Top Secret material; or

(h) A cryptographic communication system authorized by the Director, National Security Agency, or other secure communications circuits approved by the Department Security Officer.

§ 17.102 Transmission of Secret and Confidential information.

Transmission of Secret and Confidential information may be effected by:

(a) Any of the means approved for the transmission of Top Secret information except that Secret information may be introduced into the Armed Forces Courier Service only when the control of such information cannot be otherwise maintained in United States custody;

(b) Appropriately cleared Department contractors within and between the United States and its Territories provided that

(1) The designated individuals have been briefed in their responsibilities as couriers or escorts for protecting classified information; and

(2) The classified information remains under the constant custody and protection of the contractor personnel at all times;

(c) U.S. Postal Service registered mail with registered mail receipt within and between the 50 States, the District of Columbia, and Puerto Rico;

(d) U.S. Postal Service registered mail with registered mail receipt through DOD Postal Service facilities outside the 50 States, the District of Columbia, and Puerto Rico, provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection;

(e) U.S. Postal Service and Canadian registered mail with registered mail receipt between United States Government and Canadian government installations in the United States and Canada; or

(f) Government and Government contract vehicles including aircraft, ships of the U.S. Navy, civil service operated U.S. Naval ships, and ships of U.S. registry when these carriers are under appropriately cleared escort personnel. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are U.S. citizens may be designated as escorts provided the control of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. However, observation of the shipment is not required during the period it is stored in an aircraft or ship in connection with flight or sea transit, provided the shipment is loaded into a compartment that is not accessible to any unauthorized persons or in a specialized secure, safe-like container.

§17.103 Transmission of classified information to foreign governments.

Subsequent to a determination by competent authority that classified information may be released to a foreign government, it shall be transmitted only to an embassy or official agency or representative of the recipient government.

§17.104 Envelopes or containers.

(a) Whenever classified information is transmitted, it shall be enclosed in two opaque sealed envelopes or similar wrappings where size permits, except as provided below.

(b) Whenever classified material is transmitted and the size of the material is not suitable for transmission in accordance with paragraph (a) of this section, it shall be enclosed in two opaque sealed containers, such as boxes or heavy wrappings.

(c) Material used for packaging shall be of such strength and durability as to provide security protection while in transit, to prevent items from breaking out of the container, and to facilitate the detection of any tampering with the container. The outer wrappings shall conceal all classified characteristics.

§17.105 Addressing.

(a) Addresses forwarding classified information shall be specific so that couriers/messengers may easily identify the intended recipients. Use of office code numbers or such phrases in the address as ''Attention: Research Department,'' or similar aids in expediting internal routing, in addition to the organization address is encouraged.

(b) Classified written information should be folded in such a manner that the text will not be in direct contact with the inner envelope or container. A receipt form shall be attached to or enclosed in the inner envelope or container for all classified information. When written materials of different classifications are transmitted in one package, they shall be wrapped in a single inner envelope or container. A receipt listing all classified information shall be attached or enclosed. The inner envelope or container shall be marked with the highest classification of the contents.

(c) The inner envelope or container shall show the address of the receiving activity, classification, including, where appropriate, the ''Restricted Data'' marking, and any applicable special instructions. It shall be carefully sealed to minimize the possibility of access without leaving evidence of tampering.

(d) An outer or single envelope or container shall show the complete and correct address of the receiving activity and the return address of the sender.

(e) An outer cover or single envelope or container shall not bear a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks that might invite special attention to the fact that the contents are classified.

(f) Care must be taken to ensure that classified information intended only for the U.S. elements of international staffs or other organizations is addressed specifically to those elements.

§ 17.106 Receipt systems.

(a) Top Secret information shall be transmitted under a chain of receipts covering each individual who receives custody.

(b) Secret and Confidential information shall be transmitted by a receipt between activities and other authorized addressees, except that in lieu of receipts, the heads of Offices, Boards, Divisions and Bureaus may prescribe such procedures as are necessary to control effectively Secret and Confidential information.

(c) Receipts shall be provided by the transmitter of the material and the forms shall be attached to the inner envelope or cover.

(1) Receipt forms shall be unclassified and contain only such information as is necessary to identify the material being transmitted.

(2) Receipts shall be retained for at least two years.

§ 17.107 Transmission exceptions.

Exceptions to the transmission requirements for classified information may be authorized by the Department Security Officer, provided the exception affords an equal amount of protection and accountability as that provided by the requirements set forth above. Proposed exceptions that do not meet these minimum standards shall not be approved.

§ 17.108 General courier restrictions.

Appropriately cleared personnel may be authorized to escort/hand-carry classified material between their organization and an office to be visited, subject to the following conditions:

(a) The storage provisions of this regulation shall apply at all stops en route to the destination, unless the information is retained in the personal possession and constant surveillance of the individual at all times. The hand-carrying of classified information on trips that involve an overnight stopover is not permissible without advance arrangements for proper overnight storage in a Government installation or a cleared contractor's facility.

(b) Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places.

(c) When classified material is carried in a private, public, or Government conveyance, it shall not be stored in any detachable storage compartment such as automobile trailers or luggage racks.

(d) Security Programs Managers shall provide a written statement to all individuals escorting or carrying classified material aboard commercial passenger aircraft authorizing such transmission. This authorization statement may be included in official travel orders and should ordinarily permit the individual to pass through passenger control points without the need for subjecting the classified material to inspection. Specific procedures for carrying classified documents aboard commerical aircraft are contained in § 17.110. The Security Programs Managers shall ensure that employees carrying classified information abroad have obtained an official passport and other necessary documentations as required by the Department of State.

(e) Each organization shall account for all classified information carried or escorted by traveling personnel.

(f) Individuals authorized to carry or escort classified material shall be fully informed of the provisions of this subpart prior to departure from their duty station.

§ 17.109 Restrictions on hand-carrying classified information aboard commercial passenger aircraft.

Classified information shall not be hand-carried aboard commercial passenger aircraft unless:

(a) There are no other authorized means available to move the information to accomplish operational objectives or contract requirements in a timely manner.

(b) The hand-carrying has been authorized by the Department Security Officer or the Security Programs Manager or a designated Security Officer of the Office, Board, Division or Bureau concerned.

(c) The hand-carrying is accomplished aboard a U.S. carrier. Foreign carriers will be utilized only when no United States carrier is available and then the information must remain in the custody and physical control of the U.S. escort at all times.

§17.110 Procedures for hand-carrying classified information on commercial passenger aircraft.

(a) *Basic requirements.* Advance and continued coordination by the Office, Board, Division or Bureau shall be made with departure airline and terminal officials and, where possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of this issuance and Federal Aviation Administration guidance. Specifically, a determination should be made beforehand as to whether documentation described in paragraph (c) of this section, will be required. Local Federal Aviation Administration Security Officers can be of assistance in making this determination.

(1) The individual designated as courier shall be in possession of a Department picture identification card and written authorization from the Security Programs Manager of the organization concerned or the Department Security Officer to carry classified information.

(2) The courier shall be briefed as to the provisions of this subpart.

(b) *Procedures for carrying classified information.* Persons carrying classified information should process through the airline ticketing and boarding procedure in the same manner as all other passengers except for the following:

(1) The classified information being carried shall contain no metal bindings and shall be contained in sealed envelopes or other suitable containers. Should such envelopes or packages be contained in a briefcase or other carry-on luggage, the briefcase or luggage shall be routinely offered for opening and inspection for weapons.

(2) Opening or reading of the classified document by the screening official is not permitted.

(c) *Procedures for transporting classified information in large packages.* Classified information in large sealed or packaged containers shall be processed as follows:

(1) The Department official who has authorized the transport of the classified information shall notify the appropriate air carrier in advance.

(2) The passenger carrying the information shall report to the affected airline ticket counter prior to boarding, present his documentation and the package or cartons to be exempt from screening. The airline representative will be requested to review the documentation and description of the containers to be exempt.

(3) If satisfied with the identification of the passenger and his documentation, the airline official will be requested to provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the container from physical or other type inspection.

(4) If the airline officials or screening personnel refuse to permit the package to be loaded onto the aircraft without inspection, the courier will contact the appropriate Department official for further instructions.

(5) The actual loading and unloading of the information will be under the supervision of a representative of the air carrier; however, appropriately cleared personnel shall accompany the material and keep it under surveillance during loading and unloading operations. In addition, appropriately cleared personnel must be available to conduct surveillance at any intermediate stops where the cargo compartment is to be opened.

§17.111 Accountability of Top Secret information.

(a) Top Secret Control Officers and alternate Top Secret Control Officers shall be designated, in writing, by Security Programs Managers within all Offices, Boards, Divisions and Bureaus. Copies of such designations shall be forwarded to the Department Security Officer. Such officers shall be responsible for receiving, transmitting, and maintaining accountability registers for Top Secret information. They shall be selected on the basis of experience, reliability, and shall have appropriate security clearances. Further, Security Programs Managers shall ensure that written procedures concerning accountability of Top Secret information are promulgated. A copy of such procedures shall be forwarded to the Department Security Officer.

(b) All Top Secret information received or originated with the Department shall be immediately registered by an appropriate Top Secret Control

Officer or alternate. Such registering process shall include the recording of: The date the document was received and originated; the classification of the document; the number of copies; the title and description of the document; the disposition and date; the location of the document; and the serial number assigned to the document. For example, the 25th Top Secret document received within the Criminal Division during 1982 could be assigned the following Top Secret control number: CRM–82–0025.

(c) Top Secret accountability registers shall be maintained by each originating and receiving office for all Top Secret documents received or in its custody.

(d) The name and title of all individuals, including stenographic and clerical personnel, to whom information in Top Secret documents has been disclosed, and the date of such disclosure, shall be recorded. The use of a sheet of paper permanently attached to the document concerned may serve as a disclosure record or log for these purposes. Disclosures to individuals who may have had access to containers in which Top Secret infomation is stored need not be recorded on disclosure records. Disclosure records shall be retained for two years after the document concerned is transferred, downgraded or destroyed.

§ 17.112 Inventories.

Top Secret documents and material shall be inventoried at least once annually. Organizations which store large volumes of classified information may limit their annual inventory to documents and material which have been disclosed within the past year. If a storage system contains large volumes of information and security measures are adequate to prevent access by unauthorized persons, the head of the Office, Board, Division or Bureau may submit a request for a waiver of the annual inventory requirement to the Department Security Officer. However, the request must be fully justified to provide a basis for the Attorney General to approve, in writing, the waiver of these annual inventory requirements.

§ 17.113 Accountability of Secret and Confidential information.

Security Programs Managers within all Offices, Boards, Divisions, and Bureaus are responsible for ensuring that accountability procedures for Secret and Confidential information are established within their respective organizations. Such procedures shall be written and shall pertain to Secret and Confidential information originated or received by a Department component; distributed or routed to a subelement of such component; and disposed of by the component by transfer of custody or destruction. Copies of written procedures for the accountability and control of Secret and Confidential information shall be forwarded to the Department Security Officer. At a minimum, such procedures shall provide for the identification of the document.

§ 17.114 Accountability of reproduced documents.

Reproduced copies of Top Secret, Secret and Confidential documents are subject to the same accountability and controls as the original documents. (See § 17.100(b).)

§ 17.115 Working papers.

''Working papers'' are classified documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be dated when created; marked with the highest classification of any information contained therein; protected in accordance with the assigned classification; destroyed when no longer needed; and marked with a declassification or review date when placed in permanent files. Working papers shall be accounted for and controlled in the manner prescribed for a finished document of comparable classification when released by the originator or transmitted through message center channels; filed permanently; or retained more than 180 days from date of origin.

Subpart H—Disposal and Destruction of Classified Information

§17.116 Policy.

All National Security Information shall be destroyed in a manner described herein whenever the operational or historical need for the particular classified information ceases to exist. Every effort shall be made to destroy National Security Information as soon as practical for two basic reasons:

(a) First, the longer large volumes of National Security Information are existent, the greater the potential for compromise.

(b) Second, the physical and document security requirements involving National Security Information are expensive to fulfill and maintain. The smaller the amount of National Security Information in existence within the Department, the fewer storage containers and security areas are required and the smaller the budgetary allotment which must be allocated by the Department to fulfill security requirements.

§17.117 Record material.

Documentary record material made by an Office, Board, Division or Bureau of the Department in connection with the transaction of public business, and preserved as evidence of the organization, functions, policies, operations, decisions, procedures, or other activities of any Department or Agency of the government, may be disposed of or destroyed only in accordance with Offices, Boards and Divisions (OBD) Order 2710.3A, Chapter 6.

§17.118 Nonrecord material.

Nonrecord material containing classified information (including shorthand notes, used carbon paper, one-time typewriter ribbons, word processor disks, preliminary drafts, plates, records and tapes, stencils, negatives, and the like, and wastage incidental thereto) shall be destroyed, in accordance with this subpart, as soon as it has served its purpose, unless it is the subject of an ongoing mandatory review for declassification request. Prior to destruction, this material must be protected in a manner to prevent unauthorized disclosure of the information in accordance with the safeguarding procedures contained in this regulation.

§17.119 Methods of destruction.

Top Secret, Secret and Confidential classified information and material (record and nonrecord) shall be destroyed in the presence of an appropriately cleared official by burning, melting, chemical decomposition, pulping, pulverizing, shredding or other mutilation sufficient to preclude recognition or reconstruction of the classified information. Classified information stored on floppy disks or other forms of magnetic media can also be destroyed by erasure but only when unclassified information is substituted in its place.

§17.120 Records of destruction.

(a) Records of destruction are required for Top Secret and Secret information and shall be dated and signed by two officials (destruction and witnessing officials) witnessing actual destruction. If destruction is accomplished by an approved central disposal system, the destruction record shall be signed by the witnessing officials at the time the material is delivered at the facility. Records of destruction shall be maintained for a minimum of two years after which they may be destroyed. Such records shall contain the identification of the document(s) destroyed, the method of destruction used, the time and place of destruction, the reason for destruction, and the name of the destroying official and witness.

(b) The Security Programs Manager, his/her appointed Security Officer(s) when appropriate, Top Secret Control Officers or their alternates, or custodians of classified information, are authorized to destroy National Security Information. An additional person, who possesses a security clearance at the same or higher level than the classification of the material being destroyed, shall witness the destruction thereof. The destruction officials shall be trained in the operation of the equipment being used for destruction and shall ensure that destruction is accomplished in accordance with provisions of this subpart.

Subpart I—Special Access Programs

§ 17.121 Policy.

It is the policy of the Department to utilize the standard classification categories and the applicable sections of Executive Order 12356 and its implementing Information Security Oversight Office Directive to limit access to classified information on a ''need-to-know'' basis to personnel who have been determined to be trustworthy. It is also the policy to apply the ''need-to-know'' principle so that there will be no need by the Department to resort to formal special access programs which further restrict access to classified information. If it is determined a special access program should be created, a specific showing in writing must be prepared that demonstrates:

(a) Normal management and safeguarding procedures are not sufficient to limit ''need-to-know'' or access.

(b) The number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved.

(c) The safeguarding requirements of subpart E may be modified by the Attorney General as long as the modified requirements provide appropriate protection for the information.

§ 17.122 Authority for establishing special access programs.

The Attorney General may establish or continue special access programs to control access to, and distribution and protection of, particularly sensitive information originated within the Department and classified pursuant to Executive Order No. 12356. Request for such establishment shall be submitted in writing to the Department Security Officer. However, special access programs involving intelligence sources or methods, such as the Sensitive Compartmented Information Program, may be established only by the Director of Central Intelligence.

§ 17.123 Requesting the establishment or renewal of special access programs.

(a) Special access program requests shall be in writing and shall contain the information specified in § 17.124, below. Such requests shall be from the head of the Office, Board, Division or Bureau concerned and addressed to the Attorney General through the Department Security Officer. After a decision has been made concerning approval/disapproval, the original copy shall be maintained for records purposes by the Department Security Officer.

(b) Special access programs approved within the Department are required to be reviewed at least every five years by the Office, Board, Division or Bureau concerned and by the Department Security Officer.

§ 17.124 Information required in requests for special access programs.

Each special access program request, whether for establishment or renewal, shall contain the following information:

(a) Office, Board, Division or Bureau concerned (including subunit),

(b) Unclassified name or short title of the program,

(c) Relationship, if any, to other special access programs within the Department or other departments,

(d) Rationale and justification for establishment of a special access program, including the reason(s) why normal management and safeguarding procedures for classified information are inadequate,

(e) Estimated number of persons to be granted special access within the Department, in other departments, and outside the Executive Branch or U.S. Government, and

(f) All instructions pertaining to the program security requirements including, but not limited to, those governing access to program information.

§ 17.125 Identification markings and accounting for special access programs.

(a) The Department Security Officer may prescribe additional markings to identify information given protection by means of a special access program.

(b) The Department Security Officer shall account for and maintain a listing of those special access programs approved by the Attorney General. The

Director, Information Security Oversight Office, shall have non-delegable access to all such accountings.

Subpart J—Executive Branch Oversight and Policy Direction

§17.126 National Security Council.

Pursuant to the provisions of Executive Order 12356, the National Security Council shall provide overall policy direction for the Information Security Program.

§17.127 Administrator of General Services.

The Administrator of General Services is responsible for implementing and monitoring the Information Security Program. In accordance with Executive Order 12356, this responsibility has been delegated to the Director of the Information Security Oversight Office.

§17.128 Information Security Oversight Office.

(a) The Information Security Oversight Office has a full-time Director appointed by the Administrator of General Services with approval of the President. The Office is supported by a staff appointed by the Director.

(b) The Director of the Information Security Oversight Office is charged with the following principal functions that pertain to the Department:

(1) Develop, in consultation with the Department and other agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of Executive Order 12356, which shall be binding on the Department and the Offices, Boards, Divisions and Bureaus;

(2) Oversee Department actions to ensure compliance with Executive Order 12356 and the Information Security Oversight Office implementing directive;

(3) Review the Department's implementing regulations and guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this regulation or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The Department regulation or guideline shall remain in effect pending a prompt decision on the appeal;

(4) Have the authority to conduct on-site reviews of the Information Security Program of each agency that generates or handles classified information and to require of each agency such reports, information, and other cooperation as may be necessary to fulfill the Director's responsibilities. If these reports pose an exceptional national security risk, the Attorney General or the Department Security Officer may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(5) Consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the Information Security Program;

(6) Have the authority to prescribe, after consultation with the Department and affected agencies, standard forms that will promote the implementation of the Information Security Program;

(7) Report at least annually to the President through the National Security Council on the implementation of Executive Order 12356; and

(8) Have the authority to convene and chair interagency meetings to discuss matters pertaining to the Information Security Program.

§17.129 Department representatives to interagency meetings.

(a) The Counsel for Intelligence Policy is the representative of the Attorney General to interagency meetings on matters of general interest concerning information security.

(b) Concerning particular matters of information security, the Attorney General will designate a representative based on the recommendations of the Counsel for Intelligence Policy and the head of the affected Office, Board, Division or Bureau.

§17.130 Coordination with the Information Security Oversight Office.

Security Programs Managers of the Offices, Boards, Divisions and Bureaus

shall ensure that any requirements levied directly on their organization by the Information Security Oversight Office are brought to the attention of the Department Security Officer by telephone or in writing as appropriate for the situation.

Subpart K—Department of Justice Security Responsibilities

§ 17.131 General responsibilities and duties.

(a) It shall be the responsibility and duty of each officer and employee of the Department having knowledge of Classified information or material relating to the national security no matter how such knowledge was obtained to be familiar with and adhere to the provisions of this regulation concerning National Security Information and material.

(b) It shall be the responsibility of the Department Security Officer to establish and orientation program throughout the Department for the instruction and familiarization of employees with the provisions of this regulation. Such program shall initially emphasize the changes in the rules governing classification, declassification, and protection of National Security Information and material resulting from Executive Order 12356, the Information Security Oversight Office's implementing directive, and this regulation.

(c) Any employee, contractor, licensee or grantee of the Department having access to and possession of classified information is responsible for protecting it from persons not authorized access to it, to include securing it in approved equipment or facilities whenever it is not under the direct supervision of authorized persons, and meeting accountability requirements prescribed by the Attorney General through the Department Security Officer.

(d) The Department Security Officer shall establish a continuing program of security awareness for the instruction of employees regarding the protection of National Security Information and potential threats of compromise to the Department.

§ 17.132 Loss or possible compromise of classified information.

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to the Security Programs Manager designated for his/her organization. The agency that originated the information shall be notified immediately by the Security Programs Manager of the loss or possible compomise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The Office, Board, Division or Bureau under whose cognizance the loss or possible compromise occurred shall initiate an inquiry in accordance with subpart L.

§ 17.133 The Attorney General.

The Attorney General, upon request by the head of an agency or a duly designated representative, shall personally or through authorized representatives of the Department render an interpretation of Executive Order 12356, its implementing directive or this regulation with respect to any question arising in the course of its administration.

§ 17.134 Assistant Attorney General for Administration.

The Assistant Attorney General for Administration is the senior Department official having authority and responsibility to direct and administer the Department's Information Security Program (DOJ Order 990–82 (Oct. 6, 1982)). He/she will ensure effective and uniform compliance within the Department of this regulation. As such, the Assistant Attorney General for Administration has delegated primary responsibility for providing guidance, oversight, developing policy and procedures governing the Department of Justice Information Security Program to the Department Security Officer.

§ 17.135 Department Review Committee.

(a) The Department Review Committee is hereby established and is responsible for the following functions:

(1) To resolve all issues concerning implementation and administration of

Executive Order 12356, Information Security Oversight Office Directive No. 1 concerning National Security Information and this regulation, including those issues concerning overclassification, failure to declassify, and delays in declassification not otherwise resolved (the compromise of National Security Information excepted).

(2) To review all appeals of requests for record under the provisions of Mandatory Review for Declassification of Executive Order 12356 and under the Freedom of Information Act (5 U.S.C. 552) when the proposed denial is based on their continued classification under Executive Order 12356.

(3) To recommend to the Attorney General appropriate administrative sanctions to correct abuse or violation of any provision of Executive Order 12356, the Information Security Oversight Office Directive, or this regulation (the compromise of National Security Information excepted).

(4) To review, on appeal, challenges to classification actions.

(b) The voting members of the Department Review Committee shall consist of a senior representative from each of the following elements within the Department:

(1) Office of the Deputy Attorney General;

(2) Office of Legal Counsel;

(3) Criminal Division;

(4) Civil Division;

(5) Justice Management Division;

(6) Federal Bureau of Investigation;

(7) Office of Intelligence Policy and Review.

(c) The head of each component listed above will designate a voting member and an alternate in writing to the Chairman of the Department Review Committee who shall be designated by the Attorney General from among the voting members.

(d) A quorum of the Department Review Committee shall consist of the voting members or alternates from at least four of the components listed above.

(e) The Office of Information and Privacy shall provide the necessary administrative staff in support of the Department Review Committee.

[Order No. 1112–85, 50 FR 46388, Nov. 7, 1985, as amended by Order No. 1187–87, 52 FR 17752, May 12, 1987]

§17.136 The Office of Professional Responsibility.

The Office of Professional Responsibility shall investigate, or cause to be investigated, all suspected or known security violations or compromises of National Security Information detected within the Department or involving Department classified information, and shall make appropriate recommendations to the Attorney General concerning administrative and criminal sanctions.

§17.137 The Department Security Officer.

(a) There shall be a Department Security Officer within the Justice Management Division who shall serve as the Director of the Security Staff or any successor organization. It shall be the duty of the Department Security Officer, and such assistants as he/she may designate, to supervise the administration of these regulations. Except as otherwise provided in this regulation, the Department Security Officer shall also carry out the functions and exercise the authority of the Attorney General and the Department Review Committee in the administration of this regulation within the Department.

(b) As provided in Paragraph 6.c., Department Order 2600.2A, the Department Security Officer is also responsible for the development, supervision, and administration of Department Security Programs, including the promulgation of Department-wide policy and procedures and security directives.

(c) With respect to questions of law and policy that pertain to safeguarding National Security Information, the Department Security Officer shall seek advice from the Office of Intelligence Policy and Review.

§17.138 Security education.

The Department shall establish a security education program. The program established shall be sufficient to familiarize all necessary personnel with the provisions of this regulation

and to impress upon them their individual security responsibilities. The security education program shall also provide for initial, refresher, and termination briefings as required.

§ 17.139 Oversight.

A formal review to ensure compliance with the provisions of this regulation shall be conducted periodically. The audit will be performed by the Department Security Officer or such employees of the Offices, Boards, Divisions or Bureaus recommended by the head of the organization and designated, in writing, by the Department Security Officer.

§ 17.140 Heads of Offices, Boards, Divisions and Bureaus.

Pursuant to Department Order 2600.2A, the heads of Offices, Boards, Divisions and Bureaus are responsible for effective implementation within their respective organizations of all Department security regulations and programs including the Department National Security Information Program. Heads of Offices, Boards, Divisions and Bureaus or their Security Programs Managers shall immediately report any violations of the provisions of this regulation to the Department Security Officer and the Office of Professional Responsibility.

§ 17.141 Security Programs Managers.

Pursuant to Paragraph 6.d., Department Order 2600.2A, the Security Programs Managers possess the delegated responsibility for the management and coordination of the Department's Security Program within their organization. In such a capacity, the Security Programs Managers are responsible for observing, enforcing, and implementing security regulations or procedures pertaining to the classification, declassification, safeguarding, handling, and storage of classified National Security Information. Further, Security Programs Managers are responsible for ensuring that all employees are given adequate instructions in the provisions of Department security regulations and procedures. Security Programs Managers will at least annually review the requirements for access to classified information as a part of the continuous need-to-know evaluation. For employees not having a valid need-to-know for classified information, the Security Programs Manager is to initiate a memorandum to administratively withdraw or reduce the level of access authorized.

§ 17.142 Security Officers.

Security Officers are responsible to their appointing authority for implementation and administration of the Document Security Program as delegated and assigned in accordance with Paragraph 6.e. of Department Order 2600.2A.

§ 17.143 Emergency planning.

Each Office, Board, Division or Bureau shall have current plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. These plans shall include the disposition of classified information located in the United States and in foreign countries.

§ 17.144 Employees.

(a) All persons granted access to classified information in the course of their employment at the Department of Justice are required to safeguard that information from unauthorized disclosure. This nondisclosure obligation is imposed by statutes, regulations, access agreements, and the fiduciary relationships of the persons who are entrusted with classified information in the performance of their duties. The nondisclosure obligation continues after Department of Justice employment terminates. In addition, each employee having access to classified information is personally responsible for becoming familiar with and adhering to the provisions of this regulation.

(b) All employees (except those of the Federal Bureau of Investigation which has its own regulations on this matter) with access to National Security Information are required to report to the Department Security Officer any close personal or social relationship with a foreign national, including foreign press representatives. This requirement does not include contacts or relationships developed within the scope of

employment and known to the employee's supervisor. Any contacts with a foreign national which result in unofficial requests for job-related information or suspicion on the part of the employee with regard to the protection of National Security Information must also be reported.

(c) All employees of the Department (including contract employees and non-contractor personnel outside the Executive Branch) are to be aware of and comply with regulations concerning travel outside the continental United States. These regulations are summarized below:

(1) Pursuant to the provisions of Director of Central Intelligence Directive 1/20 entitled, ''Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information,'' Department personnel who have access to Sensitive Compartmented Information are required to advise the Department Security Office in writing, of any travel, whether official or unofficial, outside of the continental United States. Upon the determination of the Department Security Officer, it may be necessary that such personnel be provided a Defensive Security Briefing, a formal advisory which alerts traveling personnel to the potential for harassment, provocation, or entrapment.

(2) Employees, contractor personnel and non-contractor personnel outside the Executive Branch having access to classified information under the control of the Department are also required to advise the Department Security Officer of any travel outside of the United States and its territories as soon as the travel plan is known. The Department Security Officer will determine whether a Defensive Security Briefing is necessary based upon the foreign countries to be visited, the sensitivity of the employee's current position and the level of access to classified information.

(3) All regular or contract employees of the Department traveling to Communist-controlled countries for Government business or for personal reasons must be provided a Defensive Security Briefing whether or not they have access to classified information. The Security Programs Manager for the employee's organization is to be advised by the employee in advance of travel to allow adequate time to receive the briefing required by the sensitivity or critical nature of the employee's current position. Should an employee have particular security concerns about travel to other foreign countries, he may request guidance from the Department Security Officer.

(d) All Department of Justice employees (including contract employees) granted access to classified information in the course of their employment with the Department, shall be required to sign a nondisclosure agreement concerning the protection of national security information and a statement that they understand and shall conform to the provisions of this regulation.

(e) All employees with authorized access to Sensitive Compartmented Information shall be required to sign nondisclosure agreements containing a provision for prepublication review to assure deletion of Sensitive Compartmented Information and other classified information. Sensitive Compartmented Information is information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods. The prepublication review provision will require that Department of Justice employees who are authorized access to Sensitive Compartmented Information submit certain material, described further in the agreement, to the Department prior to its publication to provide an opportunity for determining whether an unauthorized disclosure of Sensitive Compartmented Information or other classified information would occur as a consequence of its publication.

(f) It must be recognized at the outset that it is not possible to anticipate each and every question that may arise under these agreements. The Department will endeavor to respond, however, as quickly as possible to specific inquiries by individuals concerning whether specific materials require prepublication review. Persons subject

to these requirements are invited to discuss their plans for public disclosures of information that may be subject to these obligations with authorized Department representatives at an early stage, or as soon as circumstances indicate these policies must be considered. Except as provided in paragraph (s) of this section for FBI personnel, all questions concerning these obligations should be addressed to the Counsel for Intelligence Policy, Department of Justice, 10th & Constitution Avenue, NW., Washington, DC 20530; the official views of the Department on whether specific materials require prepublication review may only be expressed by the Counsel for Intelligence Policy and persons should not act in reliance upon the views of other Department personnel.

(g) Prepublication review is required only as expressly provided for in a nondisclosure agreement. However, all persons who have had access to classified information have an obligation to avoid unauthorized disclosures of such information and are subject to enforcement actions if they disclose classified information in an unauthorized manner. Therefore, persons who have such access but are not otherwise required to submit to prepublication review under the terms of an employment or other nondisclosure agreement are encouraged to submit material for prepublication review voluntarily if they believe that such material may contain classified information. Where there is any doubt, individuals are urged to request prepublication review to avoid unauthorized disclosure and for their own protection.

(h) The nature and extent of the material that is required to be submitted for prepublication review under nondisclosure agreements is expressly provided for in those agreements. It should be clear, however, that such requirements do not extend to any materials that exclusively contain information lawfully obtained at a time when the author has no employment, contract, or other relationship with the U.S. Government or that contain information exclusively acquired outside the scope of employment.

(i) A person's obligation to submit material for prepublication review remains identical whether such person actually prepares the material or causes or assists another person, such as a ghost writer, spouse or friend, or editor in preparing the material. Material covered by a nondisclosure agreement requiring prepublication review must be submitted prior to discussing it with or showing it to a publisher, coauthor, or any other person who is not authorized to have access to it. In this regard, it should be noted that a failure to submit such material for prepublication review constitutes a breach of the obligation and exposes the author to remedial action even in cases where the published material does not actually contain Sensitive Compartmented Information or classified information. *See Snepp* v. *United States,* 444 U.S. 507 (1980).

(j) The requirement to submit material for prepublication review is not limited to any particular type of material or disclosure. Written materials include not only book manuscripts but all other forms of written materials intended for public disclosure, such as (but not limited to) newspaper columns, magazine articles, letters to the editor, book reviews, pamphlets, and scholarly papers. Because fictional treatment may convey factual information, fiction material must also be submitted if it is based upon or reflects information required to be submitted for review under the terms of a nondisclosure agreement that includes an express prepublication review provision.

(k) Oral statements are also within the scope of a prepublication review requirement when based upon written materials, such as an outline of the statements to be made. There is no requirement to prepare written materials for review, however, unless there is reason to believe in advance that oral statements may contain Sensitive Compartmented Information or other information required to be submitted for review under the terms of nondisclosure agreement. Thus, a person may participate in an oral presentation where there is no opportunity for prior preparation (e.g., news interview, panel

discussion) unless there is reason to believe in advance that such oral expression may contain Sensitive Compartmented Information or other information that must be submitted for review. This recognition of the problems inherent in oral representations does not, of course, exempt present or former employees from liability for any unauthorized disclosures of Sensitive Compartmented Information or classified information that may occur in the course of even extemporaneous oral expressions.

(l) Written materials that consist solely of personal views, opinions or judgments and do not contain or imply any statement of fact that would fall within the terms of a nondisclosure agreement requiring prepublication review, are not subject to prepublication review requirements. For example, public speeches or publication of articles on such topics as proposed legislation or foreign policy do not require prepublication review as long as the material does not directly or implicitly constitute a factual statement that falls within the purview of a nondisclosure agreement requiring prepublication review. Of course, in some circumstances the expression of ''opinion'' may in fact disclose information that requires adherence to a prepublication review obligation required under a nondisclosure agreement. Again, consultation is urged to ensure conformity to this obligation.

(m) Obviously, the purposes of prepublication review will be frustrated where the material in question already has been disseminated to unauthorized persons. In such cases, comparison of the material before and after the review would reveal to the unauthorized persons which items of information were considered to be classified and had been deleted at the Department's request. Consequently, the Department will consider a prepublication review obligation to have been breached in any case, whether or not the written material is subsequently submitted to the Department of prepublication review, where it already has been circulated to publishers or reviewers or has otherwise been made available to unauthorized persons. While the Department reserves the right to review such material for purposes of mitigating damage that may result from the disclosure of classified information, such action shall not prevent the U.S. Government and the Department from pursuing all appropriate remedies available under law as a consequence of the failure to submit the materials for prior review and any unauthorized disclosure of Sensitive Compartmented Information or classified information that may have occurred as a result.

(n) Material submitted for prepublication review will be reviewed solely for the purpose of identifying and preventing the disclosure of Sensitive Compartmented Information and other classified information. This review will be conducted in an impartial manner without regard to whether the material is critical or favorable to the Department. No effort will be made to delete embarrassing or critical statements that are unclassified. Materials submitted for review will be disseminated to other persons or agencies only to the extent necessary to identify classified information.

(o) The Counsel for Intelligence Policy (or, in the case of FBI employees, the FBI's Office of Congressional and Public Affairs) will respond substantively to prepublication review requests within 30 working days of receipt of the submission. Priority shall be given to reviewing speeches, newspaper articles, and other materials that the author seeks to publish on an expedited basis. The Counsel's decisions may be appealed to the Deputy Attorney General, who will process appeals within 15 working days of receipt of the appeal. (See §17.144(s)(3) concerning appeal procedures for FBI emplolyees.) The Deputy Attorney General's decision is final and not subject to further administrative appeal. Persons who are dissatisfied with the final administrative decision may obtain judicial review either by filing an action for declaratory relief or by giving the Department notice of their intention to proceed despite the Department's requests for deletions of classified information, and a reasonable opportunity (30 working days) to file a civil action seeking a court order prohibiting disclosure. Of course, until

any civil action is resolved, employees remain under an obligation not to disclose or publish information determined by the Government to be classified.

(p) Nothing in this subpart should be construed to alter or waive the Department's authority to seek any remedy available to it to prohibit or punish the unauthorized disclosure of classified information.

(q) A former Department of Justice employee who subsequently receives a security clearance or Sensitive Compartmented Information access approval from another department or agency is permitted to satisfy any obligation to the Department of Justice regarding prepublication review by making submissions to the department or agency that last granted the individual either a security clearance or Sensitive Compartmented Information access approval.

(r) The obligations of Department of Justice employees as described in this subpart also apply with equal force to contractors who are authorized by the Department to have access to Sensitive Compartmented Information or other classified information.

(s) The obligations of Department of Justice employees described in this subpart apply with equal force to employees of the Federal Bureau of Investigation with the following exceptions and *provisos:*

(1) Nothing in this subpart shall supersede or alter obligations assumed under the basic FBI employment agreement;

(2) FBI employees required to sign nondisclosure agreements containing a provision for prepublication review pursuant to this subpart shall submit materials for review to the Assistant Director, Office of Congressional and Public Affairs. Such individuals shall also submit questions as to whether specific materials require prepublication review under such agreements to that Office for resolution. Where such questions raise policy questions or concern significant issues of interpretation under such an agreement, the Assistant Director, Office of Congressional and Public Affairs, shall consult with the Counsel for Intelligence Policy prior to responding to the inquiry;

(3) Decisions of the Assistant Director, Office of Congressional and Public Affairs, concerning the deletion of classified information, may be appealed to the Director, Federal Bureau of Investigation, who will process appeals within 15 working days of receipt. Persons who are dissatisfied with the Director's decision may, at their option, appeal further to the Deputy Attorney General as provided in paragraph (o) of this section. Judicial review, as set forth in that paragraph, is available following final agency action in the form of a decision by the Director or, if the appeal process in paragraph (o) of this section is pursued, the Deputy Attorney General.

Subpart L—Security Violations and Administrative Sanctions

§ 17.145 Violations subject to sanctions.

(a) Officers and employees of the Department and its contractors, grantees and consultants are subject to appropriate administrative sanctions if they:

(1) Knowingly, willfully or negligently and without authorization disclose to unauthorized persons information classified under Executive Order 12356 or prior orders or compromise classified information through negligence;

(2) Knowingly and willfully classify or continue the classification of information in violation of Executive Order 12356, its implementing directives or this regulation; or

(3) Knowingly and willfully violate any other provision of Executive Order 12356, any implementing directives or this regulation.

(b) Sanctions include but are not limited to warning notices, reprimands, termination of classification authority, suspension or termination of security clearance, and as permitted by law, suspension without pay, forfeiture of pay, removal or dismissal. Sanctions will be imposed upon any person subject to these regulations and responsible for a violation specified under

this subpart as determined by the appropriate Department official upon recommendation by the Office of Professional Responsibility. In cases involving the compromise of classified information, the Attorney General, upon receiving a recommendation from the Office of Professional Responsibility, shall determine and impose appropriate sanctions.

§17.146 Reporting security violations.

Any person subject to these regulations who suspects or has knowledge of a violation pursuant to §17.145 (including the known or suspected loss or compromise of National Security Information) shall promptly report and confirm in writing the circumstances. If the loss itself is classifiable, secure telecommunications must be used for the initial report. The loss must be confirmed in writing to the Security Programs Manager of the Office, Board, Division or Bureau concerned or to that official's appropriate Security Programs Manager or representative. The Security Programs Manager of the organization under whose cognizance the loss occurred shall take the following action forthwith:

(a) Prompt notification of the violation to the Department Security Officer, to the Office of Professional Responsibility, to the origination office and to any interested department or agency, if appropriate. In the event of disagreement as to which Office, Board Division or Bureau is the cognizant agency, the Department Security Officer will promptly decide and advise the concerned Security Programs Managers by telephone.

(b) The submission of a written report to the Department Security Officer and the Office of Professional Responsibility. Such report shall include the date the violation occurred, if known; the date of the discovery of the violation; the specific identification of the information involved in the violation; the national security classification or any caveats regarding the information involved; the probability of loss or compromise; an assessment of the damage incurred from a national security standpoint; corrective measures taken; the person(s) responsible for the violation; and recommended administrative, disciplinary or legal action which should be taken. The written report should be submitted no later than ten working days after the discovery of the violation.

(c) The Department Security Officer will promptly notify the Director of the Information Security Oversight Office of any violations of §17.145(a) (1) or (2).

§17.147 Corrective action.

The Department Security Officer shall ensure that appropriate and prompt corrective action is taken whenever a violation of §17.145 occurs. The Office of Professional Responsibility shall be informed by the Department Security Officer when such violations occur.

§17.148 Administrative discrepancies.

Repeated administrative discrepancies in the marking and handling of classified documents and material such as failure to show classification authority, failure to apply internal classification markings and incorrect computation of dates for declassification, or other repeated disregard of requirements of this regulation that are determined not to constitute a violation under §17.145 may be grounds for adverse administrative action including warning, admonition, reprimand or termination of classification authority as determined appropriate by the head of the Office, Board, Division or Bureau concerned, in accordance with applicable policies and procedures.

PART 18—OFFICE OF JUSTICE PROGRAMS HEARING AND APPEAL PROCEDURES

Sec.

AUTHORITY: Secs. 802–804 of the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3701, *et seq.*, as amended (Pub. L. 90–351, as amended by Pub. L. 93–83, Pub. L. 93–